OPTIMALISASI WINDOWS FIREWALL WITH ADVANCED SECURITY DALAM MEMBANGUN KEAMANAN JARINGAN

Penerbit WADE GROUP

Optimalisasi Windows Firewall With Advanced Security Dalam Membangun Keamanan Jaringan

Penulis : Supratman Zakir, S. Kom., M. Pd., M. Kom
ISBN : 978-602-72854-7-7
Desain & Layout : Tim Kreatif WADE GROUP

Penerbit WADE GROUP --- BuatBuku.com
CV. WADE GROUP
Jl. Pos Barat Km.1 Ngimput Purwosari Babadan Ponorogo
Indonesia 63491
BuatBuku.com
waderayasa@gmail.com
INDONESIA

Cetakan Pertama, Agustus 2015

Perpustakaan Nasional: Katalog Dalam Terbitan (KDT)
88 hlm., 13,5 x 20,5 cm

KATA PENGANTAR

Alhamdulillah puji syukur kehadirat Allah SWT, Tuhan semesta alam yang begitu konsisten menganugerahkan semua kebutuhan manusia agar mampu menjalankan visi dan misinya sebagai khalifah-Nya di muka bumi. Begitu banyak rahmat dan karunia Allah yang telah dilimpahkan, setetes ilmu, segenggam kekuatan sehingga penulis mampu merampungkan buku ini sebagai salah satu ungkapan rasa terima kasih atas semua yang telah Allah anugerahkan.

Proses penyusunan buku ini cukuplah panjang dan berliku, tapi berkat bantuan dari 3 (tiga) orang bidadariku dan satu orang pangeranku yang selalu memberikan motivasi dan harapan, penyemangat, pemberi senyuman terindah, penawar hati yang lelah, penyejuk pikiran yang gerah, sehingga tulisan ini akhirnya sampai pada pembaca.

Buku ini dipersembahkan kepada pembaca terutama kepada pembaca dibidang computer teristimewa rekan-rekan pembaca yang mengeluti system keamanan computer, sebagai bukti sedikit sumbangsih yang dapat dipergunakan sebagai salah satu referensi dalam membangun keamanan jaringan computer.

Buku ini berisi tentang bagaimana kekuatan computer dalam hal ini teknologi informasi sudah menjadi kekuatan tersendiri dalam praktek berkehidupan. Jaringan computer dengan berbagai kelebihan dan kekuranganya menjadikan manusia dapat berinterkasi tanpa dibatasi oleh waktu dan tempat. Kondisi tersebut juga melahirkan ketakutan bagi manusia yaitu masalah private (kerahasiaan). Buku ini hadir bagaimana membangun

system keamanan computer dengan memnafaatkan fasilitas yang telah disiapkan oleh sebuah vendor system operasi yaitu Microsoft dengan produknya Sistem Operasi Windows Server. Pemanfaatan Windows Firewall with Advanced Security dapat dijadikan salah satu alternative dalam membangun kemanan jaringan.

Selanjutnya penulis berharap dengan hadirnya buku ini, sedikit banyaknya dapat manjadi pencerah tambahan bagi rekan-rekan pembaca dalam membangun keamanan jaringan. Terima kasih selamat membaca.

Bukittinggi, Juli 2015

Penulis

DAFTAR ISI

BAB 1

KOLONIALISME TEKNOLOGI INFORMASI

Pendahuluan

Salah satu tantangan dalam persaingan global yang semakin ketat, adalah bagaimana meningkatkan daya saing bangsa dalam meningkatkan karya-karya yang bermutu dan mampu bersaing sebagai hasil penguasaan ilmu pengetahuan, teknologi dan seni (Ipteks).

Munculnya kolonialisme baru di bidang iptek dan ekonomi menggantikan kolonialisme politik menjadikan fenomena tersendiri, dengan demikian kolonialisme kini tidak lagi berbentuk fisik, melainkan dalam bentuk informasi. Berbagai usaha dilakukan untuk mengelola informasi, sehingga informasi dapat dijadikan bahan untuk mengambil keputusan yang krusial dalam sebuah organisasi.

Perkembangan teknologi informasi merupakan salah satu bentuk usaha untuk mengelola informasi supaya dapat berdaya guna bagi organisasi. Perkembangan teknologi komputer dan jaringan (Internet) menjadi bukti begitu pentingnya pengorganisasian informasi. Pentingnya pengelolaan informasi yang profesioanal dan proporsonal terkait dengan persaingan baik secara lokal, regional maupun global.

Sehingga, diperlukan sebuah sistem pengelolaan informasi yang saat ini telah banyak diimplementasikan dalam berbagai bidang seperti, Sistem Informasi Akuntansi (SIA), Sistem Informasi Manajemen (SIM), Sistem Informasi Produksi (SIP), Sistem Informasi Sumber Daya Manusia.

Sejalan dengan perkembangan sebuah organisasi, cara penyampaian informasipun bekembang sesuai dengan perkembangan teknologi informasi. Transaksi yang sering berlangsung di tempat yang berbeda, kebutuhan informasi yang cepat untuk mengambil keputusan, keberadaan kantor-kantor cabang sebuah organisasi, prinsip kemitraan dan gangguan keamanan jika data atau informasi dikirim dalam bentuk fisik, menjadikan teknologi informasi terutama teknologi jaringan sebagai solusi jitu dan cerdas untuk diimplementasikan dalam sebuah organisasi.

Paradigma dan Transformasi Teknologi Informasi

Perkembangan teknologi jaringan juga tidak kalah pesatnya dengan teknologi-teknologi lain dalam dunia teknologi informasi, pergeseran paradigma teknologi jaringan sistem *wire* (kabel) ke teknologi nirkabel (*wireless)* menarik bagi para pengambil kebijakan organisasi untuk menggunakan teknologi tersebut.

Jaringan komputer menjadi penting bagi manusia dan organisasinya karena jaringan komputer mempunyai tujuan yang menguntungkan bagi mereka. Tujuan jaringan komputer

adalah untuk: pertama; *resource sharing* / berbagi sesumber: seluruh program, peralatan dan data yang dapat digunakan oleh setiap orang yang ada dijaringan tanpa dipengaruhi lokasi sumber dan pemakai.

Misalnya: Staff Biro Akademik mengirimkan daftar mahasiswa baru ke perpustakaan dalam bentuk print out dengan langsung mencetaknya di printer perpustakaan dari computer di Biro akademik. Atau sebaliknya staff perpustakaan mendapatkan langsung file daftar mahasiswa baru yang disimpan di komputer staff iro akademik.

Kedua; *high reliability*/kehandalan tinggi: tersedianya sumber-sumber alternative kapanpun diperlukan. Misalnya pada aplikasi perbankan atau militer, jika salah satu mesin tidak bekerja, kinerja organisasi tidak terganggu karena mesin lain mempunyai sumber yang sama. Ketiga; menghemat uang: membangun jaringan dengan komputer-komputer kecil lebih murah dibandingkan dengan menggunakan mainframe.

Data disimpan di sebuah komputer yang bertindak sebagai server dan computer lain yang menggunakan data tersebut bertindak sebagai client. Bentuk ini disebut c*lient-server*. Keempat; *scalability*/ skalabilitas: meningkatkan kinerja dengan menambahkan komputer server atau client dengan mudah tanpa mengganggu kinerja komputer server atau komputer client yang sudah ada lebih dulu.

Kelima; medium komunikasi: memungkinkan kerjasama antar orang-orang yang saling berjauhan melalui jaringan komputer baik untuk bertukar data maupun berkomunikasi. Keenam; akses informasi luas: dapat mengakses dan mendapatkan

informasi dari jarak jauh. Ketujuh; komunikasi orang-ke-orang: digunakan untuk berkomunikasi dari satu orang ke orang yang lain. Kedelapan; hiburan interaktif.

Disamping kelibihan yang diusung oleh jaringan computer terdapat juga masalah yang akan dihadapi diantaranya adalah masalah keamanan informasi yang sangat rentan untuk dicuri, dibajak ataupun dirubah oleh pihak-pihak yang tidak memiliki otoritas atau hak untuk mengakses informasi tersebut.

Untuk mengatasi permasalahan tersebut terdapat beberapa teknologi keamanan jaingan. Kemajuan yang dicapai dalam bidang pengembangan keamanan sistem operasi komputer sendiri dan utilitasnya sudah sedemikian jauh dimana tingkat performansi, kehandalan, dan fleksibilitas *software* menjadi kriteria utama dalam proses pengembanagan *software*.

Dalam teknologi informasi, telah dan sedang dikembangkan cara-cara untuk menangkal berbagai bentuk serangan semacam itu. Salah satu cara yang ditempuh mengatasi masalah ini ialah dengan menggunakan kriptografi yang menggunakan transformasi data sehingga data yang dihasilkan tidak dapat dimengerti oleh pihak ketiga.

Transformasi ini memberikan solusi pada dua masalah keamanan data, yaitu masalah privasi (*privacy*) dan keautentikan (*authentication*). Privasi mengandung arti bahwa data yang dikirimkan hanya dapat dimengerti informasinya oleh penerima yang sah. Sedangkan keautentikan mencegah pihak ketiga untuk mengirimkan data yang salah atau mengubah data yang dikirimkan.

Dengan semakin penting dan berharganya informasi serta ditunjang oleh kemajuan pengembangan teknologi jaringan *wireless* dan *software*, tentunya menarik minat para pembobol (hacker) dan penyusup (intruder) untuk terus bereksperimen guna menemukan dan mempergunakan setiap kelemahan yang ada dari konfiguarasi sistem informasi yang telah ditetapkan.

Keamanan Informasi

Masalah keamanan dan kerahasiaan data merupakan salah satu aspek yang sangat penting dari suatu sistem informasi. Hal ini sangat terkait dengan betapa pentingnya informasi tersebut dikirim dan diterima orang yang berkepentingan. Informasi akan dikirim tidak berguna lagi apabila ditengah jalan dibajak atau disadap oleh orang yang tidak berhak.

Keamanan dan kerahasiaan pada jaringan komputer saat ini menjadi isu yang sangat penting dan terus berkembang. Perusahaan *Software Microsoft* meluncurkan beberapa sistem operasi jaringan (*Network Operating System*) yang didesain untuk mengidentifikasi kebutuhan fungsional dari sebuah server. http://wss-id.org/blogs/fajar/archive/2007/10.aspx.

Salah satu kebutuhan fungsional tersebut adalah keamanan (*security).* Beberapa produk *Microsoft* untuk sistem operasi jaringan adalah *Windows NT, Windwows Server 2000, Windows Server 2003* dan yang terakhir adalah *Windwos Server 2008*

Sistem operasi jaringan yang dikeluarkan *Microsoft* yaitu *Microsof Windows Server 2008* telah banyak digunakan oleh bebagai kalangan, bisnis, pendidikan, penelitian dan lain sebagainya.

Hal ini dikarenakan sistem tersebut memiliki fitur-fitur yang mampu mengelola jaringan dengan baik salah satunya adalah kemampuan membuat *firewall* sebagai keamanan atau penangkal dari penyusup maupun para *hacker*.

Akan tetapi seiring dengan perkembangan teknologi informasi, teknologi yang digunakan para *Intruder* maupun para *hacker* juga semakin tinggi, untuk mengantisipasi hal tersebut *Microsoft* mengeluarkan sistem operasi jaringan baru yaitu *Microsoft Windows Server 2008* yang memiliki fungsionalitas lebih baik dari pendahulunya.

Advanced Security merupakan salah satu fitur pada *Windows Server 2008* yang untuk meningkatkan keamanan setiap komputer dengan cara memblok *network traffic* yang tidak diinginkan yang akan memasuki komputer tersebut.

Berbagai organisasi selalu berpacu memanfaatkan teknologi informasi dalam pengelolaan atau manajemmen organisasi untuk lebih modern dan profesional. Salah satu usaha tersebut adalah penggunaan sistem informasi dalam pengolahan data yang ditunjang dengan teknologi jaringan baik jaringan *wire* atau jaringan kabel maupun *wireless*.

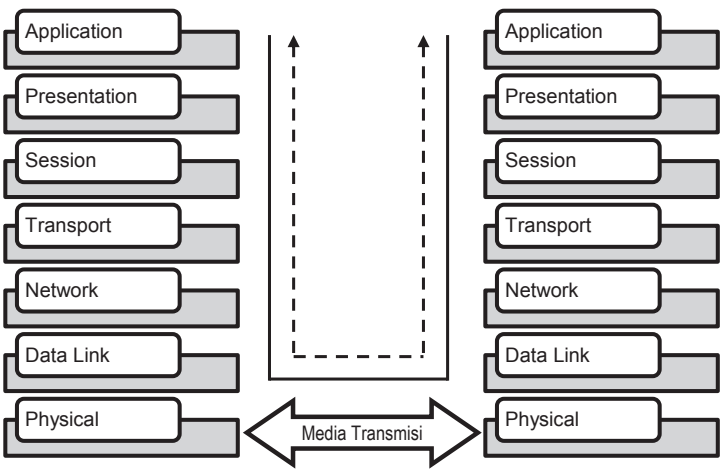
Dalam implementasinya, sistem jaringan menggunakan berbagai jenis system informasi baik *open source* maupun *proprietary*. Masalah keamanan merupakan suatu hal yang krusial, supaya data yang dikirim tidak "jatuh" kepada orang yang tidak berhak mengaksesnya.

BAB II

OPEN SYSTEM MODEL DAN PROTOCOL

Model OSI (*Open System Interconnection*)

Dalam komunikasi data, standar protokol yang terkenal yaitu OSI *(Open System Interconnection)* yang dikeluarkan oleh ISO *(International Standard Organizational)* (Abdul Kadir, 2003). Standar OSI mendefenisikan 7 (tujuh) lapisan yang dapat dilihat pada gambar dibawah ini.



Gambar : Tujuh Lapisan *(layer)* OSI

Lebih lanjut Abdul Kadir (2003), menjelaskan ketujuh *layer* atau lapisan pada OSI *(Open System Interconnection)* sebagai berikut : *Physical;* Lapisan yang menjamin pengiriman data dalam bentuk deretan bit melalui media transmisi dari satu simpul kesimpul lain. *Data Link;* Lapisan yang menjamin blok data yang mengalir ke lapisan *network* benar-benar bebas dari kesalahan.

Network; Lapisan yang mengatur rute paket data dari simpul sumber ke simpul tujuan dengan memilihkan jalur-jalur koneksi. *Transport;* Lapisan yang menyediakan hubungan yang handal antara dua buah simpul yang berkomunikasi. *Session;* Lapisan yang membentuk, memelihara dan menghentikan koneksi antara dua buah aplikasi yang sedang berjalan pada simpul-simpul yang berkomunikasi.

Presentation; Lapisan yang melakukan pengkorversian pesan (misalnya berupa enkripsi/deskripsi). *Application;* Lapisan yang menyediakan layanan komunikasi dalam bentuk program aplikasi, misalnya berupa berkas, e-mail dan pengeksekusian program jarak jauh.

Pada model OSI di atas, pemakai berinteraksi dengan sistem melalui aplikasi yang beroperasi pada apisan aplikasi. Selanjutnya aplikasi diproses melalui lapisan demi lapisan, hingga ke lapisan terbawah yang menghubungkan dua buah sistem secara fisik.

Protocol TCP/IP (*Transmission Control Protocol/Internet Protocol*)

Jika dua buah sistem ingin berkomunikasi maka harus mengikuti aturan-aturan yang dapat dipahami atau diterima oleh kedua sistem. Terlebih lagi jika kedua sistem berbeda. Aturan tersebut disebut dengan protocol. Protokol merupakan aturan atau tatacara untuk melakukan komunikasi antara dua sistem.

Menurut Abdul Kadir (2003) protokol merupakan suatu tatacara yang digunakan untuk melaksanakan pertukaran data (pesan) antara dua buah sistem dalam jaringan. Protokol dapat menangani perbedaan format data pada kedua sistem yang berbeda.

Sementara Thomas (2004) menjelaskan bahwa protokol merupakan seperangkat aturan yang menentukan format pesan antara komputer dan orang. Sedangkan protokol keamanan jaringan merupakan prosedur yang aman untuk meregulasi transmisi data antar komputer.

Transmission Control Protocol/Internet Protocol (TCP/IP) merupakan seperangkat protokol standard industri yang dirancang untuk jaringan yang besar. TCP/IP termasuk *routable,* yang berarti bahwa paket-paket dapat diarahkan *(routed)* ke subnet yang berbeda dengan memakai alamat tujuan paket (WSS-ID Team, 2008).

Protokol TCP/IP digunakan sebagai sarana komunikasi semua komputer yang terhubung ke internet. Dengan menggunakan bahasa yang sama, maka perbedaan jenis komputer dan

perbedaan sistem operasi yang digunakan tidak menjadi masalah melakukan komunikasi.

Artinya TCP/IP memungkinkan dan memberi kemudahan bagi *user* untuk mengembangkan spesifikasi sistem yang berbeda.

Secara singkat sebuah protokol komunikasi akan menangani kesalahan transmisi, mengatur *routing* dan menghantarkan data serta mengontrol transmisi. Pada arsitektur TCP/IP peneliti hanya akan membahas 2 (dua) buah protokol yaitu TCP (*Transmission Control Protocol)* dan *IP (Internet Control Protocol).*

a. TCP (*Transmission Control Protocol*)
   TCP merupakan sebuah protokol komunikasi yang menyediakan transfer data yang handal *(reliable).* TCP bersifat *connection oriented,* dan mendukung *byte stream service.*

   Connection oriented adalah sebelum pertukaran data, dua buah aplikasi pengguna TCP harus melakukan pembentukan hubungan *(Handshake)* terlebih dahulu. *Reliable* artinya TCP menerapkan proses deteksi kesalahan paket dan retransmisi sementara *byte stream* berarti paket dikirimkan dan sampai ke tujuan secara berurutan.

   Dalam kerjanya, TCP melakukan transmisi data per segmen, artinya paket data dipecah dalam sejumlah paket yang sesuai dengan ukuran paket, lalu kemudian dikirim satu persatu hingga selesai. Agar pengiriman data sampai dengan baik, maka pada setiap paket pengiriman, TCP akan menyertakan nomor seri *(sequence number).*

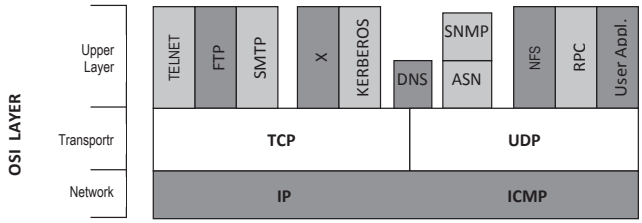
b. IP (*Internet Control Protocol*)

IP merupakan inti dari arsitektur TCP/IP, semua data yang berasal dari protokol pada layer di atas IP harus dilewatkan, diolah dan dipancarkan sebagai paket IP agar sampai ke tujuan. Dalam pengiriman data, IP memiliki sifat *unreliable, connectionless* dan *datagram delivery service*.

Unreliable berarti bahwa IP tidak dapat menjamin data yang di transmisikan sampai ke tujuan. Jika terjadi gangguan pada saat transmisi yang mengakibatkan data tidak sampai ke tujuan maka IP akan memberitahukan ke pengirim bahwa telah terjadi masalah dan paket data tidak sampai ke tujuan.

Connectionless berarti bahwa kedua belah pihak yang melakukan transmisi data tidak melakukan atau mengadakan pembentukan hubungan *(handshake)*.

Datagram delivery service berarti bahwa paket data yang dikirim merupakan paket data yang independen, artinya bawah di saat pengiriman paket data bisa saja menggunakan jalur yang berbeda. Lebih lengkapnya protokol-protokol yang terdapat pada TCP/IP dapat dilihat pada gambar berikut ini.



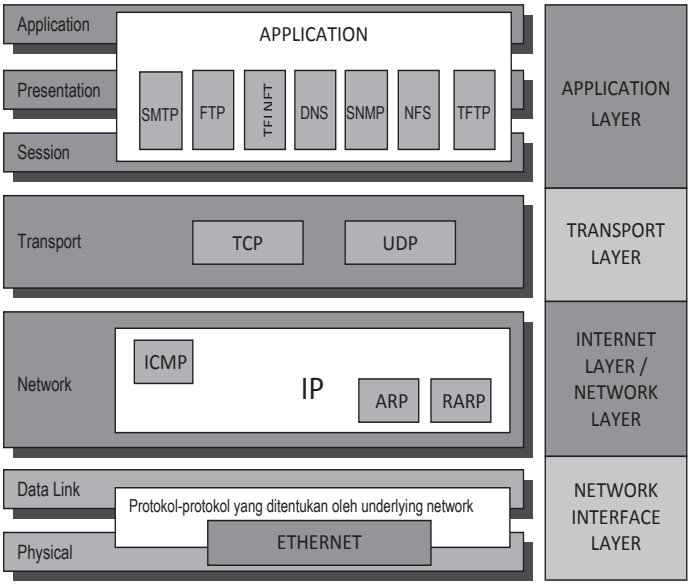
Gambar Protokol-protokol pada arsitektur TCP/IP (Onno W. Purbo, dkk, 2002)

Ket :

Telnet	: Remote Login
NFS	: Network File Server
FTP	: File Transfer Protocol
RPC	: Remote Procedure Calls
SMTP	: Simple Mail Transfer Protocol
TCP	: Transmission Control Protocol
X	: X Windows System
UDP	: User Datagram Protocol
Kerberos	: Protocol Security
IP	: Internet Protocol
DNS	: Domain Name System
ICMP	: Internet Control Message Protocol
ASN	: Abstract Syntax Notation
SNMP	: Simple Network Management Protocol

Beberapa konsep yang menjadikan TCP/IP sebuah protokol yang terkenal dan banyak digunakan adalah konsep *open system, layer, protocol* dan standarisasi.

Open system; TCP/IP merupakan sebuah protokol yang bersifat *open system,* artinya TCP/IP memiliki arsitektur yang terbuka dan memungkinkan interkoneksi dengan sistem lain. *Layer;* TCP/IP menggunakan 4 (empat) layer, dimana keempat layer tersebut merupakan 2 (dua) layer terbawah dan 3 (tiga) layer teratas pada model OSI dikombinasikan menjadi satu layer. Susuan layer pada TCP/IP dapat dibandingkan dengan model OSI seperti gambar berikut ini.



Gambar : Susunan model OSI dan Protokol TCP/IP (Onno W. Purbo, dkk, 2002)

Adapun penjelasan layer pada model OSI telah diuraikan pada pembahasan model OSI sebelumnya. Sementara untuk arsitektur TCP/IP dapat dijelaskan berikut ini.

c. Application Layer
Pada layer ini terdapat semua aplikasi atau protokol-protokol seperti: *http, ftp, telnet, smtp, snmp, dns,* dan lain-lain. Lapisan aplikasi ini yang berinteraksi langsung dengan *user*.

d. Transport Layer
Merupakan layer komunikasi data yang mengatur aliran data ke *host* tujuan. Terdapat 2 (dua) protokol penting pada layer

ini, yaitu TCP dan UDP. TCP menyediakan layanan lapisan transport untuk aplikasi, selain itu TCP juga menyediakan servis yang *reliable* atau menyediakan servis *connection oriented.*

Sementara UDP *(User Datagram Protocol)* merupakan protokol *process to process* yang menambahkan alamat port, *check sum error control* dan panjang informasi dari lapisan di atasnya serta tidak *reliable* dan bersifat *connectionless*.

e. Internet Layer / Network Layer
Protokol yang berada pada layer ini bertanggung jawab dalam proses pengiriman paket ke alamat yang tepat. Beberapa protokol yang berada pada layer ini adalah *Internet Protocol (IP), Address Resolution Protocol (ARP)* dan *Internet Control Message Protocol (ICMP).*

IP berfungsi menyampaikan paket data ke alamat yang tepat, ARP berfungsi untuk menemukan alamat *hardware* dari komputer/*host* yang terletak pada *network* yang sama dan ICMP digunakan untuk mengirimkan pesan dan melaporkan kegagalan pengiriman data.

f. Network Interface Layer
Pada layer ini terdapat penggabungan 2 (dua) layer pada model OSI yaitu *data link layer* dan *physical layer.* Pada *physical layer* terdapat *Network Interface Card NIC).* Secara keseluruhan layer ini bertanggung jawab menangani hubungan ke atau dari NIC, menentukan besar paket dan mengkonversikan IP ke alamat mesin atau sebaliknya dan pada layer ini terjadi penterjemahan sinyal listrik menjadi sinyal digital atau sebaliknya yang dimengerti oleh komputer.

BAB III

KEAMANAN JARINGAN KOMPUTER

Keamanan Jaringan

Membahas mengenai keamanan jaringan tidak lepas dari resiko yang ditimbulkan dari ancaman *(threat)* yang ada. Beberapa ancaman di antaranya adalah *virus, worm, spyware,* serangan *DoS (Denial of Services)*, pencurian informasi maupun *power failure*. Uraian selengkapnya tentang ancaman dibahas pada sub bab 2.3.2. tentang serangan pada jaringan komputer.

Menurut Harianto (2005), ancaman dapat dilakukan seseorang atau proses yang mengeksploitasi suatu keadaan yang rentan atau lemah dalam bidang keamanan yang biasa disebut dengan *vulnerability* (Kamus Komputer dan Teknologi Informasi Online, 2008). Beberapa keadaan yang dikategorikan *vulnerability* adalah lemahnya otentikasi dan otorisasi serta implementasi keamanan yang lemah. (Thomas, 2004)

Masalah keamanan dan kerahasiaan data merupakan salah satu aspek yang sangat penting dari suatu sistem informasi. Hal ini sangat terkait dengan betapa pentingnya informasi tersebut dikirim dan diterima orang yang berkepentingan. Informasi akan tidak berguna lagi apabila ditengah jalan dibajak atau disadap oleh orang yang tidak berhak.

Menurut Stalling (2002) ancaman terhadap keamanan terbagi atas dua kategori umum, yaitu ancaman pasif dan ancaman aktif. Ancaman pasif disebut juga dengan mendengarkan secara diam-diam *(Eavesdropping)*, mencakup upaya-upaya penyerang *(hacker* dan *intruder)* mendapatkan informasi yang berkaitan dengan suatu komunikasi. Sedangkan ancaman aktif mencakup beberapa modifikasi data yang ditransmisikan atau mencoba membuat sebuah data yang sedang ditransmisikan tidak sampai pada tujuan yang dituju.

Beberapa cara yang dapat digunakan untuk menangkal berbagai bentuk serangan semacam di atas adalah privasi (*privacy*) dan keotentikan (*authentication*). Privasi mengandung arti bahwa data yang dikirimkan hanya dapat dimengerti informasinya oleh penerima yang sah. Sedangkan keotentikan mencegah pihak ketiga untuk mengirimkan data yang salah atau mengubah data yang dikirimkan. (Budi Rahardjo, 2002)

Aspek/Servis Keamanan

Menurut Stalling (2002) terdapat 3 (tiga) aspek dari pada keamanan komputer dan jaringan, yaitu *privacy*, *integrity*, dan *availability*.

a. Privacy

Inti utama aspek *privacy* atau *confidentiality* adalah usaha untuk menjaga informasi dari orang yang tidak berhak mengakses. *Privacy* lebih kearah data-data yang sifatnya privat sedangkan *confidentiality* biasanya berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu (misalnya sebagai bagian dari pendaftaran sebuah

servis) dan hanya diperbolehkan untuk keperluan tertentu tersebut.

b. Integrity

Data-data bisa dimodifikasi hanya oleh pihak-pihak yang berwenang. Aspek ini menekankan bahwa informasi tidak boleh diubah tanpa seijin pemilik informasi. Adanya virus, *trojan horse*, atau pemakai lain yang mengubah informasi tanpa ijin merupakan contoh masalah yang harus dihadapi.

c. Availability.

Aspek *availability* atau ketersediaan berhubungan dengan ketersediaan informasi ketika dibutuhkan. Sistem informasi yang diserang atau dijebol dapat menghambat atau meniadakan akses ke informasi.

Selain ketiga aspek keamanan komputer dan jaringan di atas. Garfinkel dalam Budi Rahardjo (2002) menambahkan dan menjelaskan 3 (tiga) aspek lagi keamanan komputer dan jaringan, yaitu *authentication, access control* dan *non-repudiation.*

a. Authentication

Aspek *authentication* berhubungan dengan metoda untuk menyatakan bahwa informasi betul-betul asli, orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud, atau *server* yang dihubungi adalah betul-betul *server* yang dimaksud.

b. Access control

Aspek *access control* berhubungan dengan cara pengaturan akses kepada informasi. Hal ini biasanya berhubungan dengan klasifikasi data (*public, private*, *top secret*) dan *user*

(guest, admin, top manager, dsb.), mekanisme *authentication* dan juga *privacy*. *Access control* seringkali dilakukan dengan menggunakan kombinasi *userid/password* atau dengan menggunakan mekanisme lain seperti biometrics (contohnya penggunaan sidik jari dan retina mata sebagai aspek untuk mendapatkan hak akses).

c. Non-repudiation
Aspek ini menjaga agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi.

Serangan pada Jaringan Komputer

Serangan lewat jaringan adalah serangan yang memanfaatkan koneksi antar komputer sebagai media utamanya. Biasanya penyerang mengumpulkan data sistem saat korbannya terhubung ke jaringan. Metode lain adalah menanam program kecil ke dalam sistem jika korban tidak intensif menggunakan jaringan , dan akan aktif saat jalur jaringan dibuka.

Menurut Abdul Kadir (2003) terdapat beberapa jenis serangan pada sistem komputer maupun jaringan, yaitu *virus, spyware, worm, root kit, spam, phishing, DoS (denial of service), Sniffer, Spoofing*, *Man-In-The-Middle Attack* dan *Trojan Horse* .

a. Virus
Virus merupakan penggalan kode yang dapat menggandakan dirinya sendiri dengan cara menyalin kode dan menempelkan ke berkas program yang dapat dieksekusi. Selanjutnya salinan virus ini akan menjadi aktif manakala program yang terinfeksi dijalankan.

b. Spyware

Spyware memiliki tingkat bahaya yang jauh lebih rendah dibanding virus, akan tetapi *spyware* tetap harus diwaspadai. Pasalnya serangan ini bisa mencuri data penting di sebuah PC tanpa disadari korbannya. Jalur *internet* adalah media utama untuk menanam *spyware.*

c. Worm

Worm merupakan program yang dapat menggandakan dirinya sendiri dan menulari komputer yang terhubung dalam jaringan. Berbeda dengan *virus, worm* merupakan sebuah program komputer kecil yang bisa menyebar tanpa harus menumpang pada file tertentu (otonom).

Media penyebarannya juga masih menggunakan jaringan, baik lokal maupun internet. Beberapa *worm* diciptakan untuk melumpuhkan jaringan, tetapi ada juga yang dibuat untuk mencuri data (*Sobig & Mydoom*) dan menghapus file (*Explore ZIP worm*).

d. Root Kit

Root Kit sebenarnya bukan sebuah program yang berbahaya, karena diciptakan untuk melindungi hak paten bagi produk hiburan digital seperti CD *Audio* dan *DVD*. Hanya saja seiring berjalannya waktu, *Root Kit* disalahgunakan pihak tertentu untuk meraup keuntungan. *Root Kit* yang sudah dimodifikasi bisa masuk ke dalam sistem operasi dengan hak akses *administrator*. Akibatnya, pemilik *Root Kit* memiliki kontrol penuh terhadap PC korbannya.

Bahayanya lagi, *Root Kit* pandai menyembunyikan diri dan menyamar sebagai modul, *driver* atau bagian lain dari sistem

operasi, sehingga tidak mudah untuk menemukannya. *Root Kit* juga bisa bekerja di hampir semua sistem operasi yang ada saat ini, seperti *Microsoft Windows, Linux, Mac OS, Solaris*, dan lain-lain.

e. Spam

Spam sebenarnya tidak berbahaya, selama tidak ditumpangi oleh virus, *root kit* atau *file* berbahaya lain. Serangan yang datang lewat email ini biasanya digunakan untuk sarana penawaran produk atau jasa. Hanya saja jika terlampau banyak, maka jaringan akan menjadi sibuk oleh lalu-lintas *email* yang tidak jelas peruntukkannya.

f. *Phishing*

Phishing sebenarnya lebih cocok dimasukkan ke dalam kategori penipuan. Ini karena *phishing* sangat mudah dibuat, tetapi memiliki akibat kerugian yang cukup besar. Untuk membuat *phising*, tidak harus memiliki keahlian menjebol sistem yang canggih. Cukup memahami apa yang disebut *social engineering atau pengelabuan (mengelabui orang lain)*, atau kelemahan orang saat mengintepretasikan sebuah informasi di komputer.

g. DoS (denial of service)

Teknik ini dilaksanakan dengan cara membuat permintaan yang sangat banyak terhadap sistem sehingga sistem menjadi macet dan kemudian dengan mencari kelemahan pada sistem si pelaku melakukan serangan terhadap sistem.

Menurut Thomas (2004), metode serangan *DoS* digunakan untuk membuat sebuah *host* menjadi *overload* dengan membuat begitu banyak permintaan di mana *reguler traffic*

diperlambat atau kadang-kadang diinterupsi. Serangan *DoS* tidak sampai memasuki sebuah target, karena sasaran penyerang hanyalah membuat target menjadi *overload* dengan begitu banyak *traffic* palsu yang tidak dapat diatasi.

h. Sniffer

Teknik ini diimplementasikan dengan membuat program yang dapat melacak paket data seseorang ketika paket tersebut melintasi jaringan, menangkap *password* atau menangkap isinya. Lebih lanjut Thomas (2004) menjelaskan bahwa *sniffer* dapat mengkodekan data melalui dari paket melalui semua lapisan model OSI, penyerang dapat mencuri *username* dan *password* dan menggunakan informasi tersebut untuk menjalankan serangan selanjutnya.

i. Spoofing

Melakukan pemalsuan alamat *e-mail* atau *web* dengan tujuan untuk menjebak pemakai agar memasukkan informasi yang penting seperti *password.* Serangan ini mengeksploitasi hubungan dengan mengizinkan penyerang untuk mengasumsikan identitas *host* yang dipercaya.Menurut Thomas (2004) *Spoofing* muncul saat penyerang membuat paket dengan alamat IP berbeda untuk mengumpulkan *entry* ke sebuah sistem.

j. Man in The Middle Attack

Serangan yang satu ini sering terjadi pada pengguna jaringan yang tidak mengamankan jalur komunikasinya ketika sedang mengirim data penting. Sesuai namanya, *Man-In-The-Middle* merupakan serangan dengan cara "mendengarkan" data yang lewat saat 2 (dua) terminal sedang melakukan komunikasi dan kedua terminal tersebut

tidak dapat mengetahui adanya pihak ketiga di tengah jalur komunikasi mereka.

k. Trojan Horse

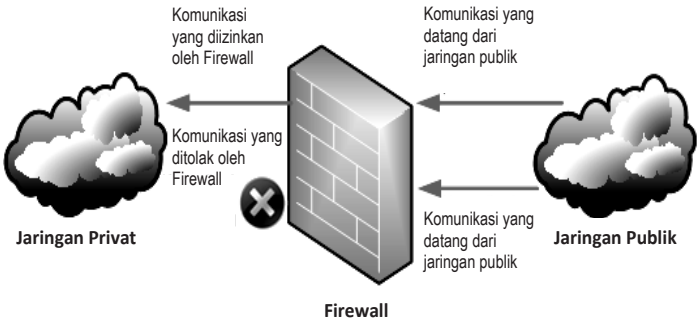
Trojan Horse merupakan program yang dirancang agar dapat digunakan untuk menyusup ke dalam sistem komputer tanpa sepengetahuan pemilik komputer. *Trojan horse* ini kemudian dapat diaktifkan dan dikendalikan dari jarak jauh atau dengan menggunakan *timer* (waktu). Akibatnya, komputer yang disisipi *trojan horse* dapat dikendalikan dari jarak jauh.

Firewall

Firewall merupakan sebuah sistem (baik *hardware* maupun *software*) yang diletakkan antara Internet dengan jaringan internal. Informasi yang keluar atau masuk harus melalui *firewall* ini. *Firewall* dapat berupa sebuah perangkat keras yang sudah dilengkapi dengan perangkat lunak tertentu, sehingga pemakai (administrator) tinggal melakukan konfigurasi dari *firewall* tersebut. *Firewall* juga dapat berupa perangkat lunak yang ditambahkan kepada sebuah server (baik *UNIX* maupun Windows *NT*), yang dikonfigurasi menjadi *firewall* (Budi Rahardjo, 2002).

Sedangkan menurut Thomas (2004) *Firewall* merupakan piranti keamanan *(security device)* yang berada pada ujung koneksi *internet* dan berfungsi sebagai *Internet Border Security Officer* atau petugas keamanan perbatasan internet. *Firewall* merupakan hukum dan pengamanan di dalam dunia maya yang tanpa hukum. *Firewall* dapat digambarkan sebagai berikut.

Sementara menurut Ahmad Muammar (2004), *Firewall* merupakan suatu cara atau mekanisme yang diterapkan baik terhadap hardware, software ataupun sistem itu sendiri dengan tujuan untuk melindungi, baik dengan menyaring, membatasi atau bahkan menolak suatu atau semua hubungan/kegiatan suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkupnya. Contoh sebuah *firewall* dapat dilihat pada gambar di bawah ini.



Gambar Contoh sebuah *Firewall* (Ahmad Muammar, 2004)

Berdasarkan beberapa defenisi di atas, dapat disimpulkan bawah *Firewall* adalah sebuah sistem yang didesain untuk mencegah akses dari pihak yang tidak berhak menuju atau dari jaringan. *Firewall* dapat diimplementasikan dalam bentuk *hardware, software*, atau kombinasi keduanya. *Firewall* biasanya digunakan untuk mencegah/mengendalikan aliran data tertentu.

Prinsip Kerja Firewall

Firewall bekerja dengan mengamati paket IP *(Internet Protocol)* yang melewatinya. Berdasarkan konfigurasi dari *firewall* maka akses dapat diatur berdasarkan IP *address, port*, dan arah informasi. Detail dari konfigurasi bergantung kepada masing-masing *firewall* (Budi Rahardjo, 2002).

Sementara menurut Thomas (2004), Firewall memeriksa aliran jaringan saat memasuki salah satu interface firewall dan menerapkan rules padanya. Pada prinsipnya firewall mengizinkan atau menolak aliran berdasarkan rules tersebut. Firewall dapat menyaring berdasarkan alamat IP sumber ataupun tujuan, protokol dan status sebuah koneksi.

Dalam menjalankan tugasnya, firewall menggunakan beberapa teknik, yaitu Service Control, Direction Control, User Control dan Behavior Control. (Ahmad Muammar, 2004).

a. Service Control
   Teknik yang digunakan berdasarkan tipe-tipe layanan yang digunakan di jaringan yang boleh diakses baik untuk kedalam (*inbound traffic)* ataupun keluar firewall *(outbound traffic)*. Biasanya firewall akan mencek IP Address dan juga nomor port yang di gunakan baik pada protokol TCP dan UDP.

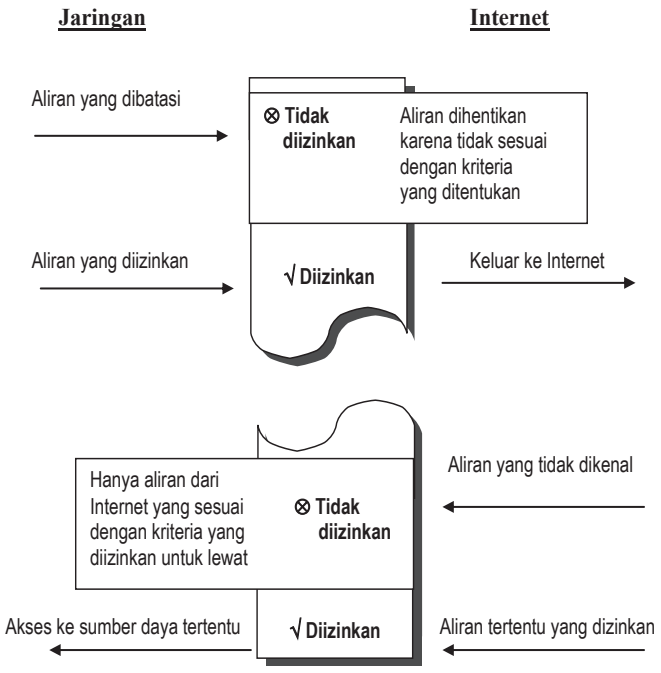
b. Direction Control
   Teknik yang digunakan berdasarkan arah dari berbagai permintaan (*request*) terhadap layanan yang akan dikenali dan diizinkan melewati *firewall*.

c. *User Control*
   Berdasarkan pengguna/*user* untuk dapat menjalankan suatu layanan, artinya ada *user* yang dapat dan ada yang tidak dapat menjalankan suatu servis, hal ini di karenakan *user* tersebut tidak diizinkan untuk melewati *firewall*. Biasanya digunakan untuk membatasi *user* dari jaringan lokal untuk mengakses keluar, tetapi bisa juga diterapkan untuk membatasi terhadap pengguna dari luar.

d. Behavior Control
   Berdasarkan seberapa banyak layanan itu telah digunakan. Misal, *firewall* dapat memfilter *e-mail* untuk menanggulangi/mencegah *spam*.

Dari definisi di atas dapat disimpulkan bawah firewall memungkinkan untuk melakukan network translation dari IP personal internal ke alamat IP publik. Walaupun firewall mampu menahan serangan bukan berarti keamanan dapat dijamin seratus persen.

Mekanisme kerja firewall secara umum dapat dilihat pada gambar berikut ini.



Gambar Operasi *Firewall* (Thomas, 2004)

Dari gambar di atas, Thomas (2004) menjelaskan bahwa peran utama *firewall* adalah memeriksa paket dan menyaring paket yang secara umum menerapkan *rules* dan fitur-fitur sebagai berikut :

a. Menolak aliran jaringan yang masuk dan keluar berdasarkan sumber atau tujuan

b. Menolak aliran *traffic* jaringan berdasarkan isi; *firewall* dapat menyaring aliran jaringan untuk isi yang dapat diterima seperti *file-file* yang berisi *virus*.

c. Mengizinkan koneksi ke jaringan internal.

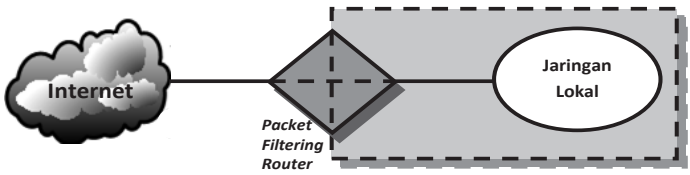
d. Melaporkan aliran jaringan dan kegiatan *firewall*; sebagian besar *fiewall* menggunakan mekanisme laporan tertentu untuk kegiatan *firewall* seperti apa yang dikerjakan *firewall* itu sendiri dan siapa yang memasuki jaringan.

Tipe-tipe Firewall

Menurut Ahmad Muammar (2004), terdapat 3 (tiga) tipe *firewall* yaitu *Packet Filtering Router, Application-Level Gateway* dan *Circuit-level Gateway*.

a. Packet Filtering Router
   Packet Filtering diaplikasikan dengan cara mengatur semua paket IP baik yang menuju, melewati atau akan dituju oleh paket tersebut. Pada tipe ini paket tersebut akan diatur apakah akan di terima dan diteruskan atau di tolak. Penyaringan paket ini di konfigurasikan untuk menyaring paket yang akan ditransfer secara dua arah (baik dari dan ke jaringan lokal).

   Aturan penyaringan didasarkan pada *header IP* dan *transport header*, termasuk juga alamat awal (IP) dan alamat tujuan (IP), protokol *transport* yang digunakan (UDP,TCP), serta nomor *port* yang digunakan. Tipe ini dapat dilihat pada gambar sebagai berikut :



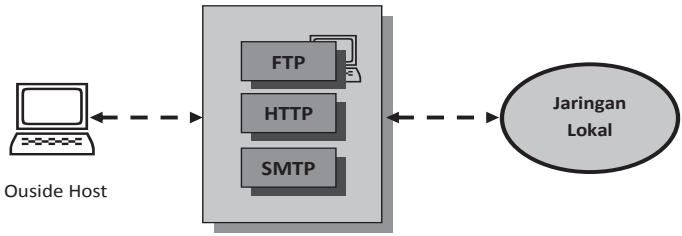
Gambar *Packet Filtering Router* (Ahmad Muammar, 2004)

b. Application-Level Gateway

Application-level Gateway yang biasa juga di kenal sebagai *proxy server* yang berfungsi untuk memperkuat/menyalurkan arus aplikasi. Tipe ini akan mengatur semua hubungan yang menggunakan layer aplikasi baik itu FTP, HTTP, dll.

Cara kerjanya adalah apabila ada pengguna yang menggunakan salah satu aplikasi seperti *FTP* untuk mengakses secara *remote*, maka *gateway* akan meminta *user* memasukkan alamat *remote host* yang akan di akses.

Saat pengguna mengirimkan *user ID* serta informasi lainnya yang sesuai, maka *gateway* akan melakukan hubungan terhadap aplikasi tersebut yang terdapat pada *remote host*, dan menyalurkan data di antara kedua titik. Apabila data tersebut tidak sesuai maka *firewall* tidak akan meneruskan data tersebut atau menolaknya. Tipe ini dapat digambarkan seperti gambar sebagai berikut :



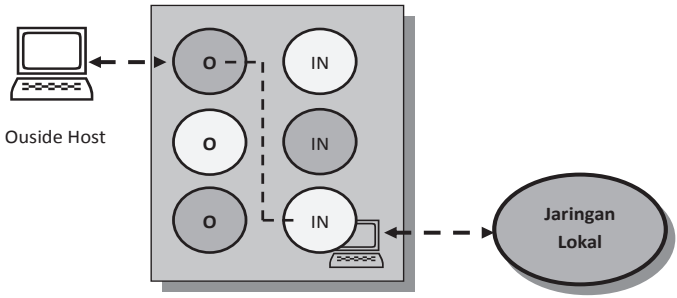
Gambar *Application-Level Gateway* (Ahmad Muammar, 2004)

c. Circuit-level Gateway

Merupakan sistem yang berdiri sendiri, atau juga dapat merupakan fungsi khusus yang terbentuk dari tipe *application-level gateway*. Tipe ini tidak mengijinkan koneksi *TCP end to end* (langsung).

Cara kerja dari tipe ini adalah *gateway* akan mengatur kedua hubungan *TCP* tersebut, 1 antara dirinya (*gateway*) dengan *TCP* pada pengguna lokal (*inner host*) serta 1 lagi antara dirinya (*gateway*) dengan TCP pengguna luar (*outside host*).

Saat dua buah hubungan terlaksana, gateway akan menyalurkan *TCP segment* dari satu hubungan ke lainnya tanpa memeriksa isinya. Fungsi pengamanannya terletak pada penentuan hubungan mana yang diizinkan. Penggunaan tipe ini biasanya dikarenakan administrator percaya dengan pengguna internal (*internal users).* Tipe ini dapat digambarkan seperti sebagai berikut.



Gambar *Circuit Level Gateway* (Ahmad Muammar, 2004)

Keterbatasan Firewall

Firewall merupakan komponen yang penting untuk mengamankan jaringan yang berkaitan dengan integritas data atau otentikasi trafik dan kerahasian jaringan internal. Dalam implementasinya *firewall* memiliki beberapa keterbatasan (Thomas, 2004) sebagai berikut :

a. *Firewall* tidak dapat mendukung kebijakan *password* atau mencegah penyalahgunaan pemakaian *password.*

b. *Firewall* tidak efektif untuk mencegah resiko-resiko keamanan non-teknis seperti *social engineering.*

c. *Firewall* merupakan wadah dari banyak *traffic* karena *firewall* memfokuskan *traffic* dan keamanan dalam satu tempat sehingga berpotensi mengalami gangguan.

Evaluasi Sistem Keamanan Jaringan

Meski sebuah sistem informasi sudah dirancang memiliki perangkat pengamanan, dalam operasi masalah keamanan harus selalu dimonitor.

Menurut Budi Rahardjo (2002), hal ini disebabkan oleh beberapa hal, antara lain.

a. Ditemukannya *security hole* (lubang keamanan) yang baru. *Software* dan *hardware* biasanya sangat kompleks sehingga tidak mungkin untuk diuji seratus persen. Kadang-kadang ada lubang keamanan yang ditimbulkan oleh kecerobohan implementasi.

b. Kesalahan konfigurasi. Kadang-kadang karena lalai atau alpa, konfigurasi sebuah sistem kurang benar sehingga menimbulkan lubang keamanan. Misalnya *mode* (*permission* atau kepemilikan) dari berkas yang menyimpan *password* secara tidak sengaja diubah sehingga dapat diubah atau ditulis oleh orang-orang yang tidak berhak.

c. Penambahan perangkat baru (*hardware* atau *software*) yang menyebabkan menurunnya tingkat *security* atau berubahnya metoda untuk mengoperasikan sistem. Operator dan administrator harus belajar lagi. Dalam masa belajar ini banyak hal yang jauh dari sempurna, misalnya *server* atau *software* masih menggunakan konfigurasi awal dari vendor.

Sumber Security Hole

Lubang keamanan (*security hole*) dapat terjadi karena beberapa hal; salah disain (*design flaw*), salah implementasi, salah konfigurasi, dan salah penggunaan (Budi Rahardjo, 2002).

a. Salah Desain *(Design Flaw)*.
   Lubang keamanan yang ditimbulkan oleh salah disain umumnya jarang terjadi. Akan tetapi apabila terjadi sangat sulit untuk diperbaiki. Akibat disain yang salah, meskipun diimplementasikan dengan baik, kelemahan dari sistem akan tetap ada. Contoh lubang keamanan yang dapat dikategorikan kedalam kesalahan disain adalah disain urutan nomor (*sequence numbering*) dari paket TCP/IP.

   Kesalahan ini dapat dieksploitasi sehingga timbul masalah yang dikenal dengan nama "*IP spoofing",* yaitu sebuah host memalsukan diri seolah-olah menjadi host lain dengan membuat paket palsu setelah mengamati urutan paket dari host yang hendak diserang.

b. Implementasi yang kurang baik
   Lubang keamanan yang disebabkan oleh kesalahan implementasi sering terjadi. Banyak program yang diimplementasikan secara terburu-buru sehingga kurang cermat dalam pengkodean sehingga menimbulkan *hole* pada sistem.

c. Salah Konfigurasi
   Meskipun program sudah diimplementasikan dengan baik, masih dapat terjadi lubang keamanan karena salah konfigurasi. Kesalahan konfigurasi ini biasanya dilakukan

oleh *administrator*. Contoh masalah yang disebabkan oleh salah konfigurasi adalah *administrator* mengaktifkan *services* yang tidak diperlukan, seperti berkas yang semestinya tidak dapat diubah oleh pemakai secara tidak sengaja menjadi "*writeable*".

Apabila berkas tersebut merupakan berkas yang penting, seperti berkas yang digunakan untuk menyimpan *password*, maka efeknya menjadi lubang keamanan.

d. Salah penggunaan
Salah penggunaan program dapat juga mengakibatkan terjadinya lubang keamanan. Beberapa bentuk kesalahan ini adalah menggunakan program-program versi beta yang masih banyak mempunyai kelemahan dan kekurangan pada program tersebut

Pengujian Keamanan Sistem

Salah satu cara untuk mengetahui kelemahan sistem adalah dengan menyerang diri sendiri dengan paket-paket program penyerang (*attack*) yang dapat diperoleh di Internet. Dengan menggunakan program dapat diketahui apakah sistem rentan dan dapat dieksploitasi oleh orang lain

Banyaknya hal yang harus dimonitor, administrator dari sistem membutuhkan *automated tools* atau perangkat pembantu otomatis, yang dapat membantu menguji atau mengevaluasi keamanan sistem yang dikelola. Untuk sistem yang berbasis Windows terdapat program yang dapat digunakan untuk menguji keamanan sistem, salah satunya adalah program

Ballista. Sementara untuk sistem yang berbasis UNIX terdapat Cops, Tripwire dan Satan/Saint.

Selain program-program (*tools*) yang terpadu (*integrated*) seperti di atas, ada banyak program yang dibuat oleh hackers untuk melakukan "coba-coba" (Budi Rahardjo, 2002). Beberapa program uji coba tersebut adalah.

a. Crack
   Program untuk menduga atau memecahkan password dengan menggunakan sebuah atau beberapa kamus (*dictionary*). Program crack ini melakukan *brute force* cracking yaitu kegiatan mencoba mengenkripsikan sebuah kata yang diambil dari kamus, dan kemudian membandingkan hasil enkripsi dengan password yang ingin dipecahkan.

   Bila belum sesuai, maka ia akan mengambil kata selanjutnya, mengenkripsikan, dan membandingkan kembali. Hal ini dijalankan terus menerus sampai semua kata di kamus dicoba.

b. Land dan Latierra
   Program yang dapat membuat sistem Windows 95/NT menjadi macet (*hang, lock up*). Program ini mengirimkan sebuah paket yang sudah di "*spoofed*" sehingga seolah-olah paket tersebut berasal dari mesin yang sama dengan menggunakan port yang terbuka.

c. Ping-o-Death
   Sebuah program (ping) yang dapat meng-*crash*-kan Windows 95/NT dan beberapa versi Unix.

d. Winuke
   Program untuk memacetkan sistem berbasis Windows

Mengamankan Sistem Jaringan

Pada umunya, pengamanan dapat dikategorikan menjadi dua jenis: pencegahan (*preventive*) dan pengobatan (*recovery*). Usaha pencegahan dilakukan agar sistem informasi tidak memiliki lubang keamanan, sementara usaha-usaha pengobatan dilakukan apabila lubang keamanan sudah dieksploitasi.

Menurut Budi Rahardjo (2002), pengamanan sistem informasi dapat dilakukan melalui beberapa layer yang berbeda. Misalnya di layer *"transport",* dapat digunakan "*Secure Socket Layer*" (SSL). Metoda ini umum digunakan untuk server web.

Secara fisik, sistem dapat juga diamankan dengan menggunakan "*firewall*" yang memisahkan sistem dengan Internet. Penggunaan teknik enkripsi dapat dilakukan di tingkat aplikasi sehingga data-data tidak dapat dibaca oleh orang yang tidak berhak.

Beberapa hal yang dapat dilakukan untuk mengamankan jaringan adalah mengatur akses kontrol, menutup servis yang tidak digunakan, memasang proteksi, pemasangan *firewall*, memantau adanya serangan pada sistem, mengamati *log file, backup* secara rutin dan penggunaan enksrpsi (Budi Rahardjo, 2002).

a. Mengatur akses kontrol
   Salah satu cara yang umum digunakan untuk mengamankan

sistem adalah dengan mengatur akses ke informasi melalui mekanisme "*authentication*" dan *"access control"*. Implementasi dari mekanisme ini antara lain dengan menggunakan "*password*". Setelah proses *authentication*, pemakai diberikan akses sesuai dengan level yang dimilikinya melalui sebuah *access control.*

Access control ini biasanya dilakukan dengan mengelompokkan pemakai dalam "*group*". Ada *group* yang berstatus pemakai biasa, ada tamu, dan ada juga *administrator* atau *super user* yang memiliki kemampuan lebih dari *group* lainnya.

b. Menutup servis yang tidak digunakan
Seringkali sistem (perangkat keras dan/atau perangkat lunak) diberikan dengan beberapa servis dijalankan sebagai default. Servis tersebut tidak semuanya dibutuhkan. Untuk mengamankan sistem, servis yang tidak diperlukan di server (komputer) tersebut sebaiknya dimatikan. Sudah banyak kasus yang menunjukkan abuse dari servis tersebut, atau ada lubang keamanan dalam servis tersebut akan tetapi sang administrator tidak menyadari bahwa servis tersebut dijalankan di komputernya.

c. Memasang proteksi / *Firewall*
Untuk lebih meningkatkan keamanan sistem informasi, proteksi dapat ditambahkan. Proteksi ini dapat berupa filter (secara umum) dan yang lebih spesifik adalah firewall. Firewall merupakan sebuah perangkat yang diletakkan antara Internet dengan jaringan internal. Informasi yang keluar atau masuk harus melalui firewall ini.

Tujuan utama dari firewall adalah untuk menjaga (*prevent*) agar akses (kedalam maupun ke luar) dari orang yang tidak berwenang (unauthorized access) tidak dapat dilakukan.

d. Memantau adanya serangan pada sistem
Sistem pemantau (*monitoring system*) digunakan untuk mengetahui adanya tamu tak diundang (*intruder*) atau adanya serangan (*attack*). Nama lain dari sistem ini adalah "*intruder detection system"* (IDS). Sistem ini dapat memberitahu administrator seperti melalui e-mail.

e. Mengamati *log file*
Sebagian besar kegiatan penggunaan sistem dapat dicatat dalam berkas yang biasanya disebut "*log file"* atau "*log*" saja. Berkas log ini sangat berguna untuk mengamati penyimpangan yang terjadi. Kegagalan untuk masuk ke sistem (*login*), misalnya, tersimpan di dalam berkas *log*. Untuk itu para administrator diwajibkan untuk rajin memelihara dan menganalisa berkas log yang dimilikinya.

f. *backup* secara rutin
Seringkali tamu tak diundang (*intruder*) masuk ke dalam sistem dan merusak sistem dengan menghapus berkas-berkas yang dapat ditemui. Jika *intruder* ini berhasil menjebol sistem dan masuk sebagai *super user* (*administrator*), maka ada kemungkinan dia dapat menghapus seluruh berkas. Untuk itu, adanya backup yang dilakukan secara rutin merupakan sebuah hal yang esensial

g. Penggunaan enkripsi
Salah satu mekanisme untuk meningkatkan keamanan adalah dengan menggunakan teknologi enkripsi. Data-

data yang kirimkan diubah sedemikian rupa sehingga tidak mudah disadap. Banyak servis di Internet yang masih menggunakan "*plain text*" untuk *authentication*, seperti penggunaan pasangan *userid* dan *password*. Informasi ini dapat dilihat dengan mudah oleh program penyadap atau pengendus (*sniffer*).

BAB IV

Sistem Operasi Windows Server

Windows Server 2008 dierkenalkan di Indnesia pada tangal 4 Februari 2008. *Microsoft Windows Server 2008* menyediakan banyak layanan dan fasilitas jaringan yang dapat digunakan. Dalam hal ini *Microsoft Windows Server 2008* mengoptimalkan teknologi-teknologi penting yang mampu menambahkan nilai, baik bagi jaringan yang baru maupun jaringan yang sudah ada.

Beberapa fitur dan tambahan tersebut diantaranya: *The Windows Server core installation option of Windows Server 2008, New and improved server management tools, Identity and Access (IDA) enhancements to Active Directory, Clustering enhancements, Terminal Services enhancement, Network Access Protection (NAP), Internet Information Services 7.0, Deployment tools.*

Dalam tesis ini, penulis tidak membahas fitur-fitur tambahan yang dibawa oleh *Windows Server 2008* di atas, akan tetapi lebih memfokuskan pada fitur sudah ada pada generasi sebelumnya yaitu *Windows Firewall with Advanced Security.*

Protocol Pada Windows Server 2008

Beberapa protokol yang umum digunakan pada sistem operasi sebelumnya, juga digunakan pada sistem perasi Windows server 2008, seperti :

a. *Transmission Control Protocol/Internet Protocol* TCP/IP
   Pembahasan mengenai protokol TCP/IP telah dibahas pada sub bab 2.2.

b. *Internet Protocol Security (IPSec)*
   Internet Protocol Security (IPsec) adalah sebuah *framework* dengan *open standard* untuk melindungi komunikasi dengan menggunakan *cryptographic security services*.

Menurut Dikshie Fauzi (1993), IPSec adalah sekumpulan ekstensi dari keluarga protokol IP. IPSec menyediakan layanan kriptografi untuk keamanan transmisi data. Layanan ini termasuk *confidentiality, integrity*, *authenticity*, dan *anti replay*.

a. *Confidentiality*, untuk meyakinkan bahwa sulit untuk orang lain tetapi dapat dimengerti oleh penerima yang sah bahwa data telah dikirimkan. Contoh: Kita tidak ingin tahu seseorang dapat melihat password ketika login ke *remote* server.

b. *Integrity*, untuk menjamin bahwa data tidak berubah dalam perjalan menuju tujuan.

c. *Authenticity*, untuk menandai bahwa data yang dikirimkan memang berasal dari pengirim yang benar.

d. *Anti Replay*, untuk meyakinkan bahwa transaksi hanya dilakukan sekali, kecuali yang berwenang telah mengizinkan untuk mengulang.

Secara teknis, IPsec terdiri atas dua bagian utama. Bagian pertama mendeskripsikan dua protokol untuk penambahan header pada paket yang membawa security identifier, data mengenai *integrity control,* dan informasi keamanan lain. Bagian kedua berkaitan dengan protokol pembangkitan dan distribusi kunci (Angga Danimartiawan, dkk, 2005).

a. AH (*Authentication header*), AH menyediakan layanan *authentication*, *integrity*, dan *replay protection*, namun tidak dengan *confidentiality*. AH juga melakukan pengamanan terhadap header IP.

b. ESP (*Encapsulated security payload*), ESP menyediakan layanan *authentication*, *integrity*, *replay protection*, dan *confidentiality* terhadap data (ESP melakukan pengamanan terhadap segala sesuatu dalam paket data setelah *header*).

Menurut Narenda Wicaksono (2008), pada *Firewall with Advanced Security, IPsec* menyediakan berbagai *connection security services* untuk *network traffic*. Setiap servis dapat dikonfigurasikan untuk diterapkan kepada suatu *network traffic* dengan cara membuat suatu *connection security rule* di *Windows Firewall with Advanced Security* yang mengidentifikasi karakteristik dari *network traffic* yang dilindungi. Beberapa *service* tersebut diantaranya adalah :

a. *Source authentication*
Source authentication memastikan bahwa setiap komputer yang berpartisipasi di dalam suatu koneksi menerima

bukti bahwa komputer yang lain (secara opsional *user* di komputer yang lain) betul-betul entitas yang sesuai. Otentikasi melibatkan setiap komputer untuk memberikan suatu bentuk kredensial kepada komputer yang lain yang dapat dibuktikan dari sumber yang benar.

b. Data integrity

Data integrity memastikan bahwa paket yang diterima identik dengan paket yang dikirimkan, dan tidak rusak atau dimodifikasi pada saat transit. Sebuah network packet yang merupakan bagian dari *network connection* menyertakan *cryptographic hash* dari paket tersebut. *Hash* tersebut dikalkulasi oleh komputer pengirim, dienkripsi dan disertakan dalam paket.

Komputer penerima mengkalkulasi *hash*-nya sendiri pada packet yang diterima, dan lalu, setelah *hash* yang disertakan didekripsi, dibandingkan kedua nilainya. Apabila mereka cocok, paket tersebut diterima dan diproses. Apabila tidak cocok, maka paket tersebut rusak atau mungkin dimodifikasi pada saat transit, lalu packet tersebut di-drop.

c. *Data confidentiality*

Data confidentiality memastikan bahwa informasi yang disertakan dalam network connection tidak dapat diakses atau dibaca oleh komputer atau user yang tidak diauthorisasi Ketika dispesifikasikan, setiap *network packet* yang merupakan bagian dari *network connection* memiliki data *payload* yang dienkripsi.

Dikshie Fauzi (2002), menjelaskan cara kerja IPSec yang dapat dibagi dalam lima tahap, yaitu:

a. Memutuskan menggunakan IPSec antara dua titik akhir di internet

b. Mengkonfigurasi dua buah *gateway* antara titik akhir untuk mendukung IPSec

c. Inisialisasi *tunnel* IPSec antara dua *gateway*

d. Negosiasi dari parameter IPSec antara dua *gateway*

e. Mulai melewatkan data

Walaupun protokol IPSec memiliki fungsionalitas yang tinggi, akan tetapi tetap memiliki beberapa kelemahan. Berikut merupakan kelibihan dan kelemahan yang dimiliki oleh IPSec menurut Angga Danimartiawan, dkk (2005).

1. Kelebihan IPSec
   a. IPsec dapat melindungi protokol apa pun yang berjalan di atas IP dan pada medium apa pun yang dapat digunakan IP, sehingga Ipsec merupakan suatu metode umum yang dapat menyediakan keamanan komunikasi melalui jaringan komputer

   b. IPsec menyediakan keamanan secara transparan, sehingga dari sisi aplikasi, user tidak perlu menyadari keberadaannya

   c. IPsec dirancang untuk memenuhi standar baru IPv6 tanpa melupakan IPv4 yang sekarang digunakan.

   d. Perancangan IPsec tidak mengharuskan penggunaan algoritma enkripsi atau hash tertentu sehingga jika algoritma yang sering digunakan sekarang telah

dipecahkan, fungsinya dapat diganti dengan algoritma lain yang lebih sulit dipecahkan.

2. Kelemahan IPSec
   a. IPsec terlalu kompleks, penyediaan beberapa fitur tambahan dengan menambah kompleksitas yang tidak perlu.

   b. Beberapa dokumentasinya masih mengandung beberapa kesalahan, tidak menjelaskan beberapa penjelasan esensial, dan ambigu.

   c. Beberapa algoritma default yang digunakan dalam IPsec telah dapat dipecahkan/dianggap tidak aman (misalnya DES yang dianggap tidak aman dan MD5 yang telah mulai berhasil diserang). Algoritma penggantinya telah tersedia dan administrator sistem sendiri yang harus memastikan bahwa mereka menggunakan algoritma lain untuk mendapatkan keamanan yang lebih tinggi.

Group Policy Object

Group Policy adalah teknologi yang tersedia sebagai bagian dari implementasi sebuah *Service Active Directory Domain*. Ketika member komputer terhubung ke sebuah *Active Directory Domain*, mereka secara otomatis mengambil dan menerapkan *Group Policy Objects (GPO)* dari *domain controller*. GPO adalah kumpulan setting yang dapat dibuat oleh domain administrator, dan lalu diterapkan pada *computer group* ataupun *user group* di dalam organisasi (Narenda Wicaksono, 2008)

Konfigurasi settings dan *rules* yang diterapkan pada komputer di organisasi disimpan di dalam *Group Policy objects (GPO)* yang dimaintain di *domain controller* dari suatu *Active Directory domain*. GPO tersebut secara otomatis di-*download* oleh setiap komputer yang ditentukan ketika mereka terhubung ke *domain*. Lalu, GPO tersebut digabungkan dengan *local GPO* yang tersimpan dalam komputer, dan lalu diterapkan pada konfigurasi yang aktif pada komputer tersebut.

Menurut Narenda Wicaksono (2008), GPO yang dikonfigurasikan mencakup beberapa dari *basic Windows Firewall with Advanced Security settings* yang sering ditemukan dalam enterprise GPO setting, seperti:

a. Setiap *local firewall setting* yang dibuat oleh user ataupun *local administrator* akan diabaikan.

b. Memastikan bahwa *firewall* telah diaktifkan untuk *network traffic* yang spesifik dan tidak dapat dinonaktifkan.

c. Komputer tersebut tidak akan menampilkan *notification* ketika Windows *Firewall with Advanced Security* memblok suatu program yang mencoba mengakses suatu *port*.

Windows Firewall with Advanced Security

Tujuan dari konfigurasi *Windows Firewall with Advanced Security* adalah untuk meningkatkan keamanan setiap komputer dengan cara memblok *network traffic* yang tidak diinginkan yang akan memasuki sebuah komputer. *Network traffic* yang tidak cocok dengan *rule set* dari *Windows Firewall with Advanced Security* akan di drop.

Selain itu juga mengharuskan suatu *network traffic* yang diperbolehkan agar dilindungi dengan menggunakan otentikasi atau enkripsi. Kemampuan untuk mengelola *Windows Firewall with Advanced Security* dengan menggunakan *Group Policy* memudahkan administrator untuk menerapkan setting yang konsisten agar tidak mudah dicapai oleh *user*.

Windows Firewall with Advanced Security mengkombinasikan *host-based firewall* dan *Internet Engineering Task Force (IETF)-compliant,* implementasi dari *Internet Protocol security (IPsec)* (Tutang, 2008).

Sebagai sebuah *host-based firewall*, *Windows Firewall with Advanced Security* berjalan pada setiap komputer yang menjalankan *Windows Server 2008* atau *Windows Vista* untuk memberikan proteksi *local* dari serangan pada jaringan yang mungkin dapat melewati *perimeter network firewall*, ataupun serangan yang berasal dari dalam organisasi.

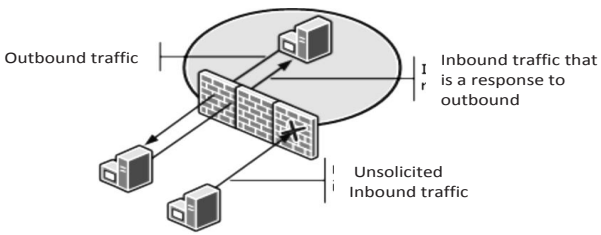
Windows Firewall with Advanced Security juga menyediakan *computer-to-computer connection security* berbasis *IPsec* yang membantu anda melindungi *network data* dengan cara mengeset *rules* sehingga dibutuhkan autentikasi, *integrity checking*, ataupun enkripsi ketika komputer-komputer di dalam organisasi anda bertukar data. *Windows Firewall with Advanced Security* bekerja pada trafik *Internet Protocol* version 4 (IPv4) dan trafik IPv6 (Fajar Faturrahman, 2008).

Host Firewall

Windows Firewall with Advanced Security menyertakan *komponen host-based firewall* yang berfungsi sebagai batas proteksi untuk

local computer, yang memonitor dan membatasi informasi yang dipertukarkan antara komputer dan network yang terhubung atau Internet. Pada *Windows Vista* dan *Windows Server 2008, host firewall* di *Windows Firewall with Advanced Security* dinyalakan secara otomatis secara *default*, dengan *inbound network traffic* diblok, dan seluruh *outbound traffic* di-*allow* (Narenda Wicaksono, 2008).

Secara *deault, Firewall* memiliki memiliki prinsip kerja meng-*allow* semua *Ourbound Network Traffict* dan mem-*block Inbount Network Traffic*. Prinsip kerja dari sebuah *firewall* dapat diperlihatkan pada gambar 2.9 berikut:



Gambar Prinsip kerja *Host Firewall* (Narenda Wicaksono, 2008)

Narenda Wicaksono (2008), menguraikan sistem kerja dari pada *host firewall* sebagai berikut :

a. *Network traffic* terdiri dari paket atau *stream of packets* yang dikirim dari sebuah *source port* dari satu komputer ke *destination port* di komputer yang lain.

b. Sebuah *port* hanyalah suatu nilai integer di dalam *network packet* yang mengidentifikasi program di sisi pengirim ataupun penerima pada suatu koneksi.

c. Secara umum, hanya satu program yang *listen* di suatu *port* pada suatu waktu. Untuk *listen* di suatu *port,* program tersebut mendaftarkan dirinya dan *port number* dimana program tersebut akan *listen* kepada sistem operasi.

d. Ketika sebuah paket tiba di *local computer*, sistem operasi memeriksa *destination port number*, dan lalu memberikan *content* dari paket tersebut ke program yang telah mendaftarkan diri untuk memakai *port* tersebut.

e. Ketika menggunakan protokol TCP/IP, suatu komputer dapat menerima *network traffic* yang dialamatkan oleh suatu *transport protocol* yang spesifik, seperti TCP atau UDP, dan pada suatu *port* yang diberi nomor dari 1 sampai 65.535.

Windows Firewall with Advanced Security bekerja dengan memeriksa s*ource* dan *destination address, source* dan *destination ports*, dan *protocol number* dari suatu paket, lalu membandingkannya dengan suatu rule yang telah didefinisikan oleh administrator. Apabila suatu *rule* cocok dengan sebuah *network packet,* lalu sebuah action yang ditentukan pada rule (untuk meng-allow atau mem-blok paket tersebut) diambil.

Pada *Windows Server 2008*, fungsionalitas di *Windows Firewall with Advanced Security* diperluas untuk menyertakan dukungan untuk meng-*allow* atau mem-*block network packets* berdasarkan apakah mereka diproteksi oleh autentikasi IPsec atau enkripsi.

BAB V

IMPLEMENTASI WINDOWS FIREWALL WITH ADVANCED SECURITY

Lingkungan Implementasi

Pada bagian ini menjelaskan bagaimana mengonfigurasikan komputer menjalankan skenario untuk *Windows Firewall with Advanced Security*. Konfigurasi yang akan didesain bukan untuk merefleksikan praktek desain terbaik ataupun konfigurasi ideal yang disarankan untuk sebuah *network security.*

Semua konfigurasi yang akan diimplementasikan, termasuk *IP Address* serta semua parameter konfigurasi lainnya didesain berjalan hanya untuk keperluan implementasi kajian laboratorium.

Adapun beberapa peralatan yang dibutuhkan (peralatan dibahwah ini bukan keharusan, yang penting peralatan yang akan dipakai dapat menjalankan Sistem Operasi Windows Server 2008) dalam menjalankan skenario pembangunan keamanan jaringan dengan memanfaatkan *Windows Firewall with Advanced Security* adalah sebagai berikut :

Perangkat Keras (Hardware)

a. Komputer Server
   Processor Intel XEON Core 2 Duo 4 Ghz, Hard disk SATA 2 x 80 GB, DVD ROM, Memory DDR2 4 GB, Display Card 512 MB, Ethernet Card 2 buah, Monitor LCD 17 inch, Keyboard + Mouse

   Komputer *server* adalah sebuah komputer yang menjalankan sistem operasi *Windows Server 2008* dan dikonfigurasikan untuk menjalankan fungsi-fungsi keamanan jaringan seperti *Windows Firewall with Advanced Security* serta *policy* dan *rule-rule* yang mendukung keamanan sebuah jaringan.

b. Komputer Client
   Processor Intel Core 2 Duo 2,4 Ghz, Memory DDR2 1 GB, DVD Multi, Harddisk 160 GB, Display Card 128 MB Shared, Ethernet Card, Monitor LCD 17 Inch, Keyboard + Mouse

   Komputer *client* adalah komputer yang menjalankan sistem operasi *Windows Vista Ultimate* yang dikonfigurasikan sebagai *user* dan diarahkan untuk dihubungkan ke domain yang digunakan pada *server*. Dalam penelitian ini peneliti menggunakan domain www.stainonline.ac.id.

Perangkat Lunak (Software)

Sistem Operasi *Windows Server 2008* yang diinstal pada komputer *server*. Sistem Operasi *Windows Vista Ultimate* yang diinstal pada komputer *client*.

Perangkat Jaringan

Switch 24 *port*. Kabel jaringan dan Konektor RJ-45

Instalasi Sistem Operasi Windows Server 2008

Instalasi sistem operasi adalah kegiatan pertama yang dilakukan dari tahapan implementasi. Sistem operasi *Windows Server 2008* diinstal pada komputer *server*. Adapun tahapan yang perlu diperhatikan pada kegiatan instalasi ini adalah sebagai berikut :

a. Menset *Local Administrator Account Password*

b. Menkonfigurasi *network* (kartu jaringan) dengan menggunakan setting sebagai berikut :
   - *IP Address* : 192.168.0.1
   - *Subnet mask* : 255.255.255.0
   - *Default Gateway* : kosongkan
   - *DNS Server Address* : kosongkan

c. Instal *Active Directory* dengan menggunakan setting sebagai berikut :
   - Buat domain baru (www.stainonline.ac.id), bagian ini juga dapat dikonfigurasikan pada program aplikasi yang digunakan seperti pada WampServer dan PHP.
   - Beri *password* untuk semua *user account*.
   - Buat *user* baru pada domain www.stainonline.ac.id, lalu beri *password*

- Tambahkan *user* yang telah dibuat ke group *Domain Administrators*

Instalasi Sistem Operasi Windows

Terdapat beberapa hal yang penting diperhatikan dalam menginstal sistem operasi *Windows Vista Ultimate* sebagai berikut :

a. Beri nama *local administrator* dan set *password*

b. Beri nama komputer *user1*

c. Identifikasi *network location type* dengan *work*

d. Konfigurasi *network* (kartu jaringan) dengan setting sebagai berikut :

- *IP Adress* : 192.168.0.5
- *Subnet mask* : 255.255.255.0
- *Default Gateway* : 192.168.0.1
- *DNS Server Address* : kosongkan

Instalasi Jaringan Lokal

Hal yang perlu diperhatikan dalam tahap instalasi jaringan adalah setting *IP address* jangan sampai ada yang konflik disamping kegiatan-kegiatan lainnya, seperti pemasangan kabel dan konektor, instalasi *switch* dan lain sebagainya.

Memeriksa Default Setting

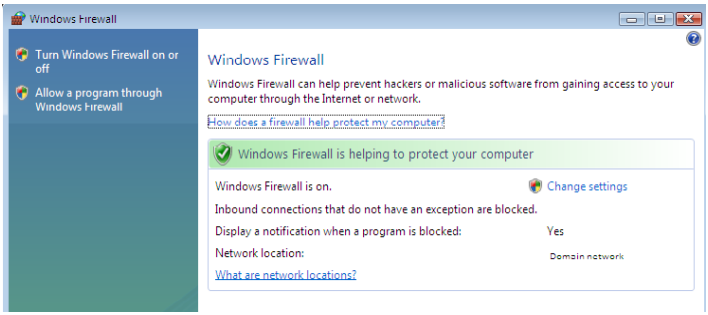
Kegiatan ini diperlukan untuk memastikan apakah *Windows Firelwall* pada komputer *server* dan *client* di *Control Panel* telah diaktifkan atau tidak. Adapun langkah-langkah baik pada komputer *server* maupun komputer *client* untuk memeriksa aktif atau tidaknya *Windows firewall* adalah sebagai berikut :

a. Klik *Start*

b. Klik *Contro Panel*

c. Klik *Windows Firewall*

d. Pada bagian *Windows Firewall Page*, setting seperti yang terlihat pada gambar 4.1. merupakan *default setting* pada setiap kali sistem operasi *windows* diinstalkan baik *Wndows Server 2008* maupun *Windows Vista Ultimate*



Gambar Jendela *Windows Firewall*

Jika fasilitas *Windows Firewall* telah aktif, maka *inbound connection* yang tidak termasuk dieksepsi (diterima) akan diblok oleh *windows firewall.*

Pada gambar terlihat bahwa setting yang digunakan adalah *Domain Network Location* karena komputer akan tergabung dengan *Active Directory Domain.*

Selanjutnya memeriksa *basic option* yang tersedia ketika menggunakan *Windows Firewall with Advanced Security*. Adapun langkah-langkah yang dilakukan adalah :

a. Buka *Windows Firewall with Advanced Security*

b. Periksa tiga panel *Firewall with Advanced Security*

- *The navigation pane* memudahkan untuk memilih *main functional area.*
- *The details pane* memperlihatkan informasi tentang *functional area.*
- *The action pane* memperlihatkan *shortcuts* kepada *task* yang tersedia dan relevan dengan *functional area*

c. Pada *Navigation Pane*, klik *Windows Firewall with Advanced Security.* lalu klik *Properties*. Terdapat empat tab, satu untuk setiap *network location profile* dan satu untuk *IPsec setting*. Perubahan yang dilakukan pada setiap *profile tab* hanya diterapkan kepada komputer ketika *network location profile* tersebut aktif. *IPsec Settings tab* memudahkan untuk mengkonfigurasi *default IPsec protocol parameters*.

d. Klik *Private Profile tab*. Untuk setiap profile, dapat diaktifkan atau menonaktifkan *firewall*, mengkonfigurasi *default firewall behavior* untuk menangani *inbound connections* dan *outbound connections* serta mengatur *logging options*

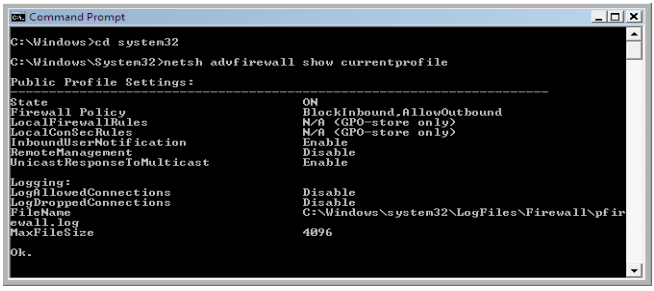
Selain dengan cara di atas, *firewall* dapat juga diperaksa melalui *nets command* dengan langkah-langkah sebagai berikut :

a. Buka *administrator command prompt*.

b. Di *command prompt*, jalankan *nets advfirewall show currentprofile*. *Advfirewall* adalah fitur baru di *nets* pada versi *Windows* ini. *firewall* dan *ipsec contexts* tetap ada, tetapi hanya disediakan untuk kompabilitas dengan *Group Policy setting* yang dibuat menggunakan versi *Windows* sebelumnya.

c. Periksa outputnya dan bandingkan dengan apa yang anda lihat sebelumnya di *Windows Firewall icon* di *Control Panel*.

   Output akan terlihat seperti gambar dibawah ini.



Gambar Tampilan *nets command*

Pada gambar di atas terlihat nilai *State, Firewall Policy*, dan *InboundUserNotification* berkorespondensi dengan *basic settings* yang telah diperiksa - *Windows Firewall icon - Control Panel* pada langkah sebelumnya.

Membuat Rule yang meng-Allow Inbound Network Traffic

Secara *default, Windows Firewall with Advanced Security* mem-*block* semua *inbound network traffic* yaitu trafik yang akan masuk dari luar atau yang akan berhubungan dengan sistem jaringan. Untuk mengaktifkan program yang memiliki ketergantungan pada trafik tersebut, maka perlu untuk membuat *rule* yang sesuai.

Ketika menggunakan program yang butuh menerima *unsolicited inbound network traffic*, maka harus membuat *rule* untuk meng-*allow traffic* tersebut melewati *firewall*. Pada bagian ini, sebagai contoh pertama, membuat sebuah *firewall rule* yang meng-*allow inbound traffic* untuk *service Telnet* melewati *firewall*, lalu *rule* tersebut diterapkan pada komputer *server* dengan menggunakan *Group Policy*.

Adapun langkah-langkah untuk membuat *firewall rule* yang meng-*allow inbound traffic* untuk suatu program adalah sebagai berikut :

a. Buka *Group Policy Management Window*, klik-kanan *Firewall Settings for WS2008 Servers*, lalu klik *Edit*.

b. Di *navigation pane*, klik *expand Computer Configuration*, lalu *expand Windows Settings,* lalu *expand Security Settings,* lalu *expand Windows Firewall with Advanced Security*, lalu *expand Windows Firewall with Advanced Security* –

c. LDAP://cn={*GUID*},cn=policies,cn=system,DC=staion line,dc=ac,dc=id

d. Klik-kanan *Inbound Rules*, lalu klik *New rule*.

e. Di *Rule Type page*, klik *Custom*, lalu klik *Next*.

f. Rule yang akan dibuat sespesifik mungkin. Itu artinya harus menspesifikasikan program dan *port*, untuk memastikan hanya program dan *port* tertentu saja yang dapat menerima *traffic*.

g. Untuk melihat semua *option* di *wizard*, pilih tipe *rule Custom*.

h. Di *text box* untuk *This program path*, ketik %systemroot%\ system32\tlntsvr.exe

i. Karena program dapat meng-*host* banyak *service*, maka sebaiknya membatasi *rule* untuk s*ervice* yang diinginkan secara spesifik

j. Disamping *Services* klik *Customize*..

k. Klik *Apply to this service*, pilih *Telnet*, klik *OK*, lalu klik *Next*

l. Di *Protocols and Ports* page, klik *Next*.

m. Membatasi *rule* untuk *port* yang spesifik dapat dilakukan hal-hal berikut.

n. Di *Scope* page, klik *Next*

o. Di *Action page*, klik *Allow the Connection*, lalu klik *Next*

p. Di *Profile page*, kosongkan *Private* dan *Public check box*. Pastikan bahwa *Domain* telah dipilih, lalu klik *Next*

q. Di *Name page*, ketik *Allow Inbound Telnet*, lalu klik *Finish*.

Ketika membuat atau mengganti *firewall rule*, yang dapat sewaktu-waktu membuat *rule set* yang meng-*allow traffic* yang tidak inginkan, atau mem-*blok traffic* yang diperlukan sering merepotkan pengguna.

Untuk membantu *troubleshooting* masalah seperti ini, *Windows Firewall with Advanced Security* dapat membuat *log file* yang berisi *entry* untuk *network connection* yang diizinkan dan *network connection* yang diblok. Pada langkah ini adalah konfigurasi GPO untuk membuat *log file* dan untuk me-*log packet* yang di-*allow* dan packet yang di-*block*.

a. Buka *Group Policy Management*

b. Pada *navigation pane*, klik-kanan *Firewall Settings for WS2008 Servers*, lalu klik *Edit*.

c. Pada *Group Policy Management Editor*, klik-kanan *node* paling atas di *navigation pane*, lalu klik *Properties*.

d. Pilih *Disable User Configuration settings check box*.

e. Pada *confirmation dialog box*, klik *Yes*, lalu klik *OK*.

f. Pada *navigation panel, expand Computer Configuration, expand Windows Settings, expand Security Settings*, lalu *expand Windows Firewall with Advanced Security*.

g. Klik-kanan *Windows Firewall with Advanced Security* - LDAP://cn={*GUID*},cn=policies,cn=system,DC=staino nline,DC=ac,DC=id, lalu klik *Properties*.

h. Pada *Domain Profile* tab, di *Logging section*, klik *Customize*.

i. Kosongkan *Not configured check box*.

j. Ganti *Log dropped packets* dari *No* ke *Yes*.

k. Ganti *Log successful connections* dari *No* ke Yes.

l. Klik *OK* dua kali untuk menyimpan seting GPO

m. Close Group Policy Management Editor

Membuat Rule yang mem-Block Outbound Network Traffic

Secara *default, Windows Firewall with Advanced Security* meng-*allow* seluruh *outbound network traffic*. Apabila organisasi melarang suatu *network program*, maka dapat dibuat *rule* agar program itu tidak dapat melakukan koneksi. Secara *default, inbound network traffic* ke suatu komputer yang tidak cocok dengan *rule* yang dijalankan akan di-*blok*.

Adapun langkah-langkah untuk mem-*block outbound network traffic* adalah sebagai berikut :

a. Pada *Group Policy Management*, klik-kanan *Firewall Settings for WS2008 Servers,* lalu klik Edit.

b. Klik *Expand Computer Configuration*, lalu *expand Windows Settings*, lalu *expand Security Settings*, lalu klik *expand Windows Firewall with Advanced Security*, -

c. LDAP://{*GUID*},cn=policies,cn=system,DC=stainonlin e,DC=ac,DC=id.

d. Klik *Outbound Rules*

e. Klik-kanan *Outbound Rules*, lalu klik *New Rule*.

f. Pada *Rule Type page*, klik *Custom*, lalu klik *Next*

g. Pada *Program page*, klik *All programs*, lalu klik *Next*

h. Pada *Protocol and Ports page*, ubah *Protocol type* ke *TCP*

i. Pada *Remote ports list*, klik *Specific Ports*, ketik 23 di *text box*, lalu klik *Next*

j. Pada *Scope page*, klik *Next*.

k. Pada *Action page*, klik *Block the connection*, lalu klik *Next*

l. Pada *Profile page*, kosongkan *Private* dan *Public check box*, lalu klik *Next*.

m. Pada *Name page*, ketik *Block Outbound Telnet*, lalu klik *Finish*

Menerapkan Basic Domain Isolation Policy

Dengan menggunakan *Windows Firewall with Advanced Security di Windows Server 2008*, dapat membuat *connection security rules* yang menspesifikasikan bahwa *traffic* harus diamankan oleh satu atau lebih fitur dari *IPsec*.

Pada *domain isolation*, dapat digunakan otentikasi untuk setiap komputer yang berhubungan dalam koneksi untuk secara postif memastikan identitas komputer lainnya.

Dengan membuat *rules* yang mengharuskan otentikasi oleh *domain member*, maka secara efektif dapat mengisolasi komputer *domain-member* tersebut dari komputer yang bukan bagian dari *domain*

Kita dapat membuat *connection security rules* untuk domain stainonline.ac.id yang akan membuat seluruh *member computers require authentication* untuk meng-*inbound network traffic*, dan *request authentication* untuk meng-*outbound traffic*.

Rule yang dibuat menggunakan *GPO* yang hanya *request inbound authentication*, dan setelah memastikan bahwa hal tersebut berjalan dengan baik, maka selanjutnya revisi ke *require inbound authentication*.

Adapun langkah-langkah untuk membuat *connection security rule* adalah sebagai berikut :

a. Pada komputer *server*, buka *Group Policy Management*, klik-kanan *Group Policy Objects*, lalu klik *New*.

b. Pada *Name*, ketik *Domain Isolation*, lalu klik *OK*.

c. Pada *navigation pane*, klik-kanan *GPO* yang baru, lalu klik *Edit*.

d. Pada *Group Policy Management Editor*, di *navigation pane*, klik-kanan node paling atas untuk *Domain Isolation GPO*, lalu klik *Properties*.

e. Pilih *Disable User Configuration settings check box*

f. Pada *Confirm Disable dialog box*, klik *Yes*, lalu klik *OK*.

g. Pada *navigation pane,* klik *expand Computer Configuration,* lalu *expand Windows Settings,* lalu *expand Security Settings,* lalu klik *expand Windows Firewall with Advanced Security* – LDAP://cn={*GUID*},cn=policies,cn=system,DC=stainonline,DC=ac,DC=id.

h. Klik-kanan *Connection Security Rules*, lalu klik *New rule*.

i. Pada *Rule Type page*, klik *Isolation*, lalu klik *Next*.

j. Pada *Requirements page*, pastikan *Request authentication for inbound and outbound connections* telah dipilih, lalu klik *Next*.

Pada bagian *production environment*, direkomendasikan untuk mengeset *request mode* terlebih dahulu dan *allow GPO* untuk melakukan propagasi secara penuh di dalam *network*. Pastikan bahwa seluruh komputer berkomunikasi dengan sukses dengan menggunakan *IPsec* sebelum mengganti *rule* ke *require mode*.

Mengeset *rule* ke *require mode* terlebih dahulu dapat membuat komputer tidak dapat berkomunikasi sampai seluruh komputer menerima dan menerapkan GPO.

Pada langkah selanjutnya, memodifikasi *rule* untuk mengganti *request mode* menjadi *require inbound authentication mode*.

a. Pada *Authentication Method page*, klik *Computer (Kerberos V5),* lalu klik *Next*.

b. Pada *Profile page*, kosongkan *Private* dan *Public check box*, lalu klik *Next*.

c. Pada *Name page*, ketik *Request Inbound Request Outbound*, lalu klik *Finish*.

Mengisolasi Server

Domain isolation membatasi *domain-member computer* untuk berkomunikasi hanya dengan *domain-member computer* yang lain.

Beberapa *server* memiliki data yang sensitif seperti, *personal data, medical records*, atau *credit card data* yang harus dijaga dengan lebih hati-hati.

Layer tambahan dari security, yang disebut *server isolation*, membatasi akses ke sensitif data tersebut hanya kepada *user* yang memiliki kepentingan yang spesifik. Kadang-kadang, data tersebut juga harus dienkripsi saat transmisi untuk mencegah *eavesdropping*.

Dengan menggunakan *Windows Firewall with Advanced Security in Windows Server 2008*, kita dapat menspesifikasikan bahwa spesifik *network connection* hanya dapat diakses oleh suatu *user*, berdasarkan *group membership*-nya. Kita juga dapat menspesifikasikan bahwa akses dibolehkan hanya bagi suatu komputer berdasarkan *computer account membership* dalam suatu *group*.

Ada 2 (dua) hal penting yang harus di konfigurasi untuk mengisolasi server, yaitu membuat *Security Group* dan memodifikasi *Firewall Rule* untuk *Require Group Membership and Encryption*

Membuat Security Group

Pada tahapan ini membuat *security group di Active Directory*. Group ini akan direferensikan oleh *firewall rule* di langkah berikutnya untuk mengontrol komputer mana saja yang dapat mengakses *server*. Adapun tahapannya adalah sebagai berikut :

a. Pada computer *server* klik *Start,* lalu klik *Server Manager*.

b. Pada *navigation pane*, klik *expand Rules*, lalu *expand Active Directory Domain Services,* lalu klik *expand Active Directory Users and Computers,* klik *expand stainonline.ac.id*, klik-kanan *Computers*, klik *New*, lalu klik *Group*.

c. Pada *New Object - Group dialog box*, ketik *Access to user1*, lalu klik *OK*.

d. Biarkan *Server Manager running*.

Memodifikasi Firewall Rule untuk Require Group Membership and Encryption

Dalam tahapan ini akan dibuat atau memodifikasi *telnet firewall rule* untuk meng-allow *Telnet traffic* hanya dari komputer yang menjadi member dari *security group* yang telah dibuat pada langkah sebelumnya. Adapun langkah-langkahnya adalah sebagai berikut :

a. Buka Group Policy Management

b. Pada *navigation pane*, di bawah *Group Policy Objects*, klik-kanan *Firewall Settings for WS2008 Servers*, lalu klik Edit.

c. Pada *Group Policy Management Editor*, *expand Windows Settings, expand Security Settings,* expand Windows Firewall with Advanced Security – LDAP://cn={*GUID*},cn=policies,cn=system,DC=stainonline,DC=ac, DC=id, lalu klik *Inbound Rules*.

d. Pada *details pane*, klik-kanan *Allow Inbound Telnet*, lalu klik *Properties.*

e. Ubah nama dengan mengetikkan *Allow Encrypted Inbound Telnet to Group Members Only*.

f. Klik *Allow only secure connections*, lalu klik *Require encryption*.

g. Klik *Users and Computers tab*.

h. Di bawah *Authorized computers*, klik *Only allow connections from these computers*, lalu klik *Add.*

i. Di *Select Computers or Groups dialog box*, ketik *Access to server*, klik *Check Names* untuk memastikan nama tersebut *resolve*, lalu klik *OK.*

j. Klik *OK* to *close the Allow Inbound Telnet Properties page*.

k. Close the Group Policy Management Editor.

Selain itu kita juga dapat menspesifikasikan *user group membership* sebagai sebuah *requirement*, selama *authentication method* yang digunakan meliputi *user authentication* dan juga *computer authentication*.

Hal ini membantu kita untuk menspesifikasikan hanya *user* yang merupakan *member* dari group yang dapat mengakses *server* yang diproteksi, dan juga ketika mereka menggunakan komputer yang merupakan *member* dari group.

User yang terotorisasi yang menggunakan komputer yang tidak terotorisasi tidak dapat mengakses *server* yang terproteksi, juga komputer yang terotorisasi tetapi digunakan oleh *user* yang tidak terotorisasi, tidak dapat mengakses *server* tersebut.

Menguji Inbound Rule untuk mem-allow network traffic

Tahapan ini merupakan pengujian terhadap *rules* yang telah dibuat untuk memblok *network traffic* dengan langkah-langkah sebagai berikut :

a. Pada komputer *server* di *Administrator: Command Prompt, run gpupdate /force.* Tunggu hingga *command* selesai.

b. Pada komputer *client* (*user1*), di *command prompt, run telnet server 25.* Eksekusi akan gagal dan mengeluarkan pesan *time out* karena *firewall di server* sekarang memblok seluruh *inbound traffic ke Telnet service* kecuali pada *port* 23.

c. Pada komputer *server* di *Administrator: Command Prompt, run tlntadmn config port=23* untuk mengembalikan *service* ke nomor *port default.*

d. Pada komputer client (*user1*), di *command prompt, run telnet server.* Eksekusi akan sukses dilaksanakan karena *firewall* meng-*allow inbound traffic* ke *Telnet service port 23*.

e. *Close* sesi *Telnet* dengan mengetikkan *exit,* lalu tekan *ENTER*

Menguji Rule untuk spesifik komputer yang di-allow inbound traffic

Untuk mengetes *Telnet connectivity* dengan *rules* yang telah dibuat sebelumnya**,** dengan langkah sebagai berikut :

a. Pada komputer *server switch* ke Administrator : Command Prompt, run gpupdate /force. Tunggu hingga command selesai.

b. Pada komputer *client (user1)* di *command prompt*, ketik *command telnet server. Command* akan gagal, karena secara *default block rule* mempunyai *precedence* yang lebih tinggi dari pada *allow rule*.

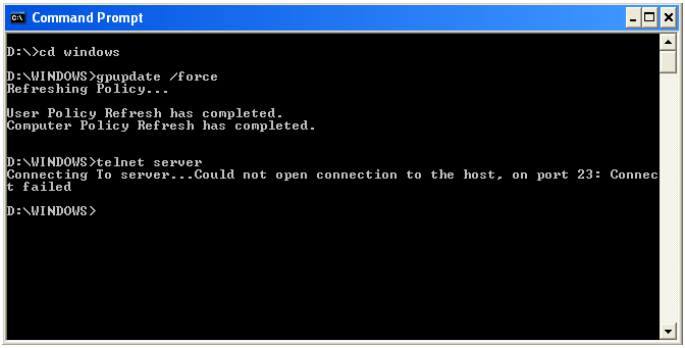
Menguji Outbound Rule untuk mem-block network traffic

Tahapan ini adalah pengujian *rules* yang telah dibuat untuk mem-*block* maupun meng-*allow network traffic*. Adapun angkah-langkahnya adalah sebagai berikut :

a. Pada komputer *user1* dibagian *administrator command prompt* jalankan *gpupdate / force*, tunggu sampai perintah dieksekusi

b. Jalankan *telnet server*

c. Koneksi akan gagal dan menampilkan pesan *error* sebagai berikut: *Connecting to server…Could not open connection to the host, on port 23: Connect failed*

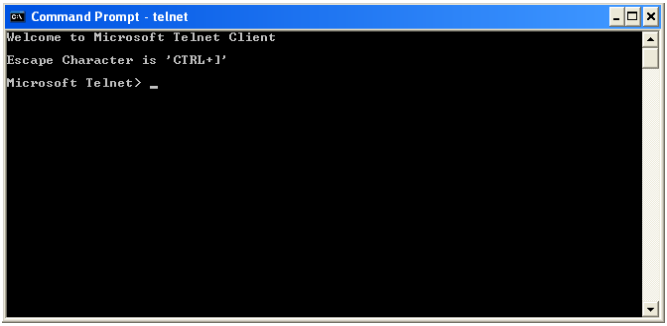


Gambar Pesan *Error* ketika *user1* ingin mengakses komputer *server*

d. Untuk bagian selanjutnya, akan menggunakan *Telnet* kembali, jadi nonaktifkan *rule* yang telah buat.

e. Pada komputer *server* di *Group Policy Management Editor*, klik-kanan *rule Block Outbound Telnet*, lalu klik *Disable Rule.*

f. Pada komputer *user1* ulangi langkah 1 dan 2 untuk memastikan *Telnet* telah aktif



Gambar Fasilitas Telnet aktif kembali

g. Ketik **exit** lalu tekan ENTER untuk mengakhiri sesi Telnet.

Menguji Rule ketika User1 bukan member group

Tahapan ini merupakan uji *client* (*user1)* yang memiliki *firewall rule* dan *connection security rule* yang memenuhi seluruh *requirement* untuk berkomunikasi dengan *server*, tetapi *user1* belum ditambahkan ke dalam *computer group* yang direferensikan di *inbound Telnet firewall rule* untuk *server*.

Adapun yang dilakukan adalah mencoba untuk *connect ke Remote Event Viewer Service* di server. Adapaun langkahnya adalah sebagai berikut :

a. Pada komputer client (*user1) Administrator: Command Prompt, run gpupdate /force*. Tunggu sampai perintah selesai dieksekusi.

b. Klik *Start*, ketik *event viewer* di *Start Search box*, lalu tekan *ENTER*.

c. Di *navigation pane Event Viewer*, klik-kanan *node* paling atas *Event Viewer (Local),* lalu klik *Connect to another computer*.

d. Di *Select Computer dialog box*, ketik server, lalu klik *OK*. Koneksi akan berhasil, karena rule yang dibuat tidak membutuhkan *group membership* ataupun *encryption* untuk *Event Viewer*.

Tetapi jika *rule* di atas belum dikonfigurasikan, maka koneksi akan mengalami kegagalan, karena *user1* belum ditambahkan ke dalam *computer group* yang direferensikan di *inbound Telnet firewall rule* untuk *server*.

BAB VI

ANALISIS IMPLEMENTASI

Analisis Implementasi

Pada bagian ini akan dibahas hasil dari tahapan implementasi yang telah dilakukan. Beberapa hal yang berkaitan dengan keamanan *server* yang telah diimplementasi dan selanjutnya dianalisis dalam penelitian ini di antaranya adalah, analisis tentang *setting default firewall*, pembuatan *rule* yang meng-*allow inbound network traffic*, pembuatan *rule* yang mem-*block outbound network traffic*, Penerapan *Basic Domain Policy* serta analisis tentang pengisolasian *server*.

Dari hasil imlementasi pemeriksaan terhadap *setting default Firewall* yang dilakukan melalui pemeriksaan melalui *Control Panel,* terlihat bahwa secara *default*, *Firewall* otomatis aktif pada sistem operasi yang terpasang.

Terlihat bahwa *Windows Firewall is on,* hal tersebut manyatakann bahwa jika *Firewall* aktif, maka *inbound connection* yang tidak termasuk dieksepsi (diterima) akan diblok oleh *windows firewall.*

Selain dengan cara pemeriksaan pada *Control Panel*, pemeriksaan *Setting Default Firewall* dapat dilakukan melalui *command promt*. Terlihat bahwa *State ON, Firewall Policy Block Inbound, Allow*

Outbound. Keadaan tersebut sama dengan hasil pemeriksaan yang dilakukan melalui *Control Panel* dan menunjukkan status yang sama.

Seperti yang telah dibahas sebelumnya bahwa secara *default, Windows Firewall with Advanced Security* mem-*block* semua *inbound network traffic* yaitu trafik yang akan masuk dari luar atau yang akan berhubungan dengan sistem jaringan. Untuk mengaktifkan program yang memiliki ketergantungan pada trafik tersebut, maka perlu untuk membuat *rule* yang sesuai. Dari hasil implementasi pembuatan *rule* untuk meng-*allow Inbound Network Traffic*.

Contoh implementasi penulis terapkan penggunaan fasilitas *Telnet* yang akan berhubungan dengan menggunakan *Port 23* sebagai *Port default*. *Rule* yang dibuat sespesifik mungkin. Itu artinya harus menspesifikasikan program dan *port*, untuk memastikan hanya program dan *port* tertentu saja yang dapat menerima *traffic*.

Secara *default*, *windows firewall* meng-*allow* semua *outbound network traffic*. Jika institusi atau organisasi menginginkan untuk melarang keluarnya informasi atau sebuah program, maka dapat dibuat *rule* agar program tersebut tidak dapat melakukan koneksi. Pada tahap implementasi, pembuatan *rule* untuk mem-*block outbound nework traffic* dilakukan dengan menggunakan fasilitas *Group Policy Management* yang ada pada *windows server 2008*.

Sementara itu, penerapan *Domain Policy* pada *domain isolation*, dimaksudkan untuk otentikasi agar setiap komputer yang berhubungan dalam koneksi dapat memastikan identitas

komputer lainnya. Dengan membuat *rules* yang mengharuskan otentikasi oleh *domain member*, maka secara efektif dapat mengisolasi komputer *domain-member* tersebut dari komputer yang bukan bagian dari *domain*.

Dari hasil penerapan *Domain Policy* dengan membuat *rule* maka kita akan dapat membuat seluruh *member computers require authentication* untuk meng-*inbound network traffic*, dan *request authentication* untuk meng-*outbound traffic*. Pembuatan *rule* dilakukan melalu fasilitas *Group Policy Management* seperti yang telah dibahas pada bab sebelumnya.

Pengisolasian *server* dimaksudkan untuk membatasi *domain-member computer* yang akan berkomunikasi hanya dengan *domain-member computer* yang diberi izin. Hal ini dilakukan karena beberapa *server* memiliki data yang sensitif seperti, *personal data, medical records*, atau *credit card data* yang harus dijaga dengan lebih hati-hati. Membatasi akses ke sensitif data tersebut hanya kepada *user* yang memiliki kepentingan yang spesifik.

Dengan menggunakan *Windows Firewall with Advanced Security in Windows Server 2008*, kita dapat menspesifikasikan bahwa spesifik *network connection* hanya dapat diakses oleh suatu *user*, berdasarkan *group membership*-nya. Kita juga dapat menspesifikasikan bahwa akses dibolehkan hanya bagi suatu komputer berdasarkan *computer account membership* dalam suatu *group*.

Impelementasi pembuatan *rule* menggunakan fasilitas *server member* dan *Group Policy Management*. Pembuatan *rule* tersebut telah dibahas pada bab sebelumnya.

Analisis Hasil Pengujian

Pada bagian ini akan dibahas hasil dari tahapan pengujian terhadap *rule* dan *policy* yang diterapkan dalam rangka membangun sistem keamanan, baik rule yang dibuat di komputer *server* maupun pada komputer *client*.

Dari hasil pengujian terhadap *rules* yang telah dibuat untuk memblok *network traffic,* terlihat bahwa ketika salah satu *service* dalam penelitian ini penulis menggunakan service *telnet*, maka eksekusi tersebut akan akan gagal dan mengeluarkan pesan *time out*, hal ini disebabkan oleh karena *firewall di server* sekarang memblok seluruh *inbound traffic ke Telnet service.*

Rule di atas dapat dirubah supaya service *telnet* dapat dieksekusi, ketika *rule* dirubah maka eksekusi akan sukses dilaksanakan karena *firewall* meng-*allow inbound traffic* ke *Telnet service port 23*.

Hasil pengujian terhadap *Outbound Rule* untuk meng-*allow network traffic,* terlihat koneksi gagal dan menampilkan pesan *error* sebagai berikut: *Connecting to server…Could not open connection to the host, on port 23: Connect failed* seperti yang ditampilkan pada saat pengujian.

Jika kita ingin mengizinkan trafik keluar dari jaringan, maka *rule* yang telah dibuat dapat dinonaktifkan. Dari hasil pengujian terlihat koneksi *telnet* akan tersambung ke *port 23*, karena *rule Block Oubound* sudah dinonaktifkan, seperti yang terlihat saat pengujian.

Sementara hasil pengujian setelah *rule* dikonfigurasikan, maka koneksi computer *client* (*user1)* akan berhasil, karena komputer

client (user1) telah ditambahkan ke dalam *computer group* yang direferensikan di *inbound Telnet firewall rule* untuk *server*.

Akan tetapi jika *rule* tidak dibuat maka komunikasi agan mengalami kegagalan, sebab computer *server* membutuhkan *group membership* ataupun *encryption* untuk *Event Viewer*.

Windows *Firewall with Advanced Security* adalah elemen yang penting dalam *defense-in-depth security strategy* untuk membantu anda mengamankan komputer dalam suatu organisasi, dan membantu dalam mitigasi melawan ancaman yang mem-*bypass* parameter *firewall* atau yang berasal dari dalam *network* itu sendiri.

Seperti yang telah dibahas sebelumnya, bahwa *Windows Firewall with Advanced Security* mengkombinasikan *host-based firewall* dan *Internet Engineering Task Force (IETF)*- yang merupakan implementasi dari *Internet Protocol security (IPsec)*.

Sebagai sebuah *host-based firewall*, *Windows Firewall with Advanced Security* berjalan pada setiap komputer yang menjalankan Windows Server® 2008 untuk memberikan proteksi dari serangan pada jaringan yang mungkin dapat melewati perimeter *netwok firewall*, ataupun serangan yang berasal dari dalam organisasi.

Windows Firewall with Advanced Security juga menyediakan *computer-to-computer connection security* berbasis *IPsec* yang membantu melindungi *network data* dengan cara mengeset *rules* sehingga dibutuhkan otektikasi, *integrity checking*, ataupun enkripsi ketika komputer-komputer di dalam suatu organisasi bertukar data.

Beberapa fitur yang dibawa oleh *Windows Firewall with Advanced Security* diantaranya :

1. *Windows Firewall with Advanced Security* menyediakan fasilitas untuk *set up basic inbound* dan *outbound fireall rules*

2. Dengan *Windows Firewall with Advanced Security* kita dapat membuat *Group Policy object* yang mengkonfigurasi *firewall setting* di setiap komputer dalam suatu domain, dan memastikan bahwa user tidak dapat mengganti setting tersebut.

3. Dengan *Windows Firewall with Advanced Security* kita dapat membuat satu *set basic domain isolation rules* yang membatasi *domain-member* komputer agar tidak menerima koneksi dari komputer yang bukan member dari domain.

4. Dengan *Windows Firewall with Advanced Security* kita dapat membuat *connection security rules* yang mengisolasi *server* penting, tempat informasi sensitif, dengan membatasi akses hanya kepada komputer yang menjadi member dari group yang disetujui.

5. Dengan *Windows Firewall with Advanced Security* kita dapat membuat *rule* yang secara spesifik menentukan komputer mana yang dapat mem-*bypass firewall*.

Dengan fasilitas-fasilitas baru tersebut *Windows Firewall with Advanced Security* pada sistem operasi *Windows Server 2008* terbukti mampu memberikan system keamanan yang baik terhadap serangan baik yang datang dari luar maupun dari dalam.

DAFTAR KEPUSTAKAAN

Abdul Kadir, (2003), Pengenalan Sistem Informasi, Yogjakarta, Andi Offset.

Adnan Basalamah, (1999), Internet & Email Security, Makalah online tidak diterbitkan www.bogor.net/idkf/idkf/network/network-security/ppt-internet-and-email-security-10-1999.ppt

Ahmad Muammar, (2004), Firewll, Kuliah Umum Ilmu Komputer, http://www.IlmuKomputer.com

Angga Danimartiawan, dkk, (2002), IPsec: Aplikasi Teknik Kriptografi untuk Keamanan Jaringan Komputer, makalah tidak diterbitkan

Budi Rahardjo (2002), Keamanan Sistem Informasi Berbasis Internet, Bandung PT. Insan Infonesia, Jakarta, PT. INDOCISC.

Didik Dwi Prasetyo (2004), Mail Server Berbasis Java pada Server Windows dan Linux, Jakarta, PT. Elex Media Komputindo..

Dikshie Fauzi (2002), Tinjauan Mekanisme dan Aplikasi Ipsec: Studi Kasus VPN, Makalah tidak diterbitkan.

Fajar Faturrahman (2008), Pengenalan Windows Server 2008, Windows Server Sistem, http://wss-id.org/blogs/fajar/archive/2007/10/21/pengenalan-windows-server-2008.aspx

Ferguson, N., and Schneier, B., (2000) A Cryptographic Evaluation of IPSec, Counterpane Internet Security, Makalah tidak diterbitkan.

Harianto Ruslim (2005), Hack Attack : Konsep, Penerapan dan Pencegahan, Jasakom, cet. I

Jethefer, Stevens, (2007), Studi dan Perbandingan Algoritma IDEA (International Data Encryption Algorithm) Dengan DES (Data Encryption Standard), Makalah tidak diterbitkan, http://www.informatika.org/~rinaldi/Kriptografi/2006-2007/Makalah1/Makalah1-005.pdf

Narenda Wicaksono (2008), Windows Server 2008 : Langkah Demi Langkah Panduan Konfigurasi Two-Node Print Server Failover Cluster, Microsft Innovation Center Institut Teknologi Bandung, http://wss-id.org/files/narenda

---------- (2008), Windows Server 2008 : Panduan Langkah demi Langkah Penerapan Policy untuk Windows Firewall with Advanced Security, Microsft Innovation Center Institut Teknologi Bandung, http://wss-id.org/files/narenda

---------- (2008), Windows Server 2008 : Windows Server Active Directory Rights Management Services Step-by-Step Guide, Microsft Innovation Center Institut Teknologi Bandung, http://wss-id.org/files/narenda

---------- (2008), Windows Server 2008 : Panduan Langkah demi Langkah: Menerapkan SSTP Remote Access, Microsft Innovation Center Institut Teknologi Bandung, http://wss-id.org/files/narenda

---------- (2008), Windows Server 2008: Panduan Setup Lisensi TS Windows Server 2008, Microsft Innovation Center Institut Teknologi Bandung, http://wss-id.org/files/narenda

---------- (2008), Windows Server 2008: Changes in Functionality from Windows Server 2003 with SP1 to Windows Server 2008, Microsft Innovation Center Institut Teknologi Bandung, http://wss-id.org/files/narenda

Nita Rahmi, (2008), Studi dan Analisis Penggunaan Key-Schedule pada Algoritma IDEA (International Data Encryption Algorithm), Makalah tidak diterbitkan, http://www.informatika.org/~rinaldi/Kriptografi/2006-2007/Makalah1/Makalah1-005.pdf

Onno W. Purbo, dkk, (2002), Buku Pintar Internet TCP/IP Standar, Desain dan Implementasi, Jakarta, PT. Elex Media Komputindo

S'To (2006), Seni Internet Hacking ReCODED, Jasakom

----------(2006), Computer Worm 1 - Secret of Underground Coding, Jasakom

---------- (2004), Mengenal Windows 2003, Jakarta, PT. Elex Media Komputindo

Stalling, William (2002), Data & Computer Communication, diterjemahkan oleh Thamir Abdul Hafedh Al-Hamdany, Jakarta, Salemba Teknika, Edisi I

Thomas, Tom (2004), Network Security First Step, terjemahan oleh Tim Penerjemah ANDI offset, Yogyakarta, Andi Offset.

Tutang (2008), Windows Server 2008 : Panduan Langkah-Langkah Opsi Instalasi Server Core pada Windows Server 2008, Microsft Innovation Center Institut Teknologi Bandung, http://wss-id.org/files/tutang

BIODATA PENULIS

Supratman Zakir, S. Kom., M. Pd., M. Kom, Lahir di sebuah desa kecil bernama Lolo Hilir Kecamatan Gunung Raya Kabupaten Kerinci Propinsi Jambi. Tahun 1990 melanjutkan pendidikan di Pondok Pesantren Modern Nurul Ikhlas Padang Panjang. Tahun 1995 memulai pendidikan Sarjana di Jurusan Teknik Komputer di Sekolah Tinggi Manajemen Informatika & Komputer (STMIK) YPTK Padang dan selesai pada tahun 2000.

Tahun 2005 menyelesaikan Pendidikan Magister di Universitas Negeri Padang (UNP) pada Jurusan Teknologi Pendidikan sebagai mahasiswa tercepat (3 semester) dengan predikat cum laude. Tahun 2006 bergabung dengan Institut Agama Islam Negeri (IAIN) Bukittinggi sebagai Dosen Tetap PNS. Mantan Ketua Jurusan Pendidikan Teknik Informatika & Komputer (2007-2010) ini saat ini menjabat sebagai Sekretaris Lembaga Penelitian dan Pengabdian Masyarakat IAIN Bukittinggi.

Beberapa penelitian yang telah dilakukan di antaranya : Evaluasi SOP Program Studi Pendidikan Bimbingan Konseling IAIN Bukittinggi (2014), Desain Sistem Informasi Administrasi UKM Berbasis Web (2012), Desan dan Implementasi Windows Configuration Wizard dalam Membangun Keamanan Jaringan (2010).

Aktif menjadi narasumber baik dilingkungan perguruan tinggi maupuan masyarakat umum, diantaranya : Narasumber Guru Cerdas dengan ICT se-Kabupaten Padang Pariaman (2013); E-Government kabupaten/kota se-Propinsi Smatera Barat (2013); Konsultan ICT-Pura Kabupaten Tanah Datar (2013); Media Pembelajaran Berbasis ICT untuk Guru Kab. Agam (2013), Konsultan ICT-Pura Kota Sawahlunto (2012), Peningkatan Kompetensi Guru PAI Kab. Agam (2012); Konsultan ICT-Pura Kota Bukittinggi (2011).

Beberapa buku yang telah diterbitkan diantaranya : Sistem Operasi; Mozaik Implementasi Teknologi Informasi; Local Website sebagai Media Pembelajaran Alternatif, Optimalisasi Windows Firewall dalam Membangun Keamanan Jaringan.

Penulis dapat dihubungi di e-mail : sefzaku@gmail.com, me@e-manza.com, http://e-manza.com